



**Обобщеномрежови модели на Data Mining
процеси за управление и защита на**

интелигентен дом

Тихомир Видев Видев

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

академик проф. дмн дтн Красимир Т. Атанасов

проф. д-р инж. Сотир Николов Сотиров

Бургас

2024

Съдържание

Използвани съкращения/чуждоезикови обозначения.....	3
БЛАГОДАРНОСТИ.....	4
УВОД.....	5
ЦЕЛ И ЗАДАЧИ НА ДИСЕРТАЦИОННИЯ ТРУД.....	7
1. ГЛАВА ПЪРВА - ОСНОВНИ ПОНЯТИЯ ОТ ТЕОРИЯТА НА ОБОБЩЕНИТЕ МРЕЖИ.....	8
1.8 ИЗВОДИ.....	8
2. ГЛАВА ВТОРА - ОБОБЩЕНОМРЕЖОВИ МОДЕЛИ НА СИСТЕМИ ЗА DATA MINING ПРОЦЕСИ В ИНТЕЛИГЕНТЕН ДОМ.....	9
2.2.1 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА КИБЕР СИСТЕМА ЗА ИНТЕЛИГЕНТЕН ДОМ С ИНТУИЦИОНИСТКА РАЗМИТА ОЦЕНКА.....	18
2.2.2 АЛТЕРНАТИВЕН МЕТОД ЗА ОЦЕНКА НА РИСКА ОТ КИБЕР АТАКА НАД УПРАВЛЕНИЕТО НА SMART HOUSE ЧРЕЗ ИНТУИЦИОНИСТКА РАЦМИТА ОЦЕНКА.....	23
2.3 ИЗВОД.....	27
3. ГЛАВА ТРЕТА - ОБОБЩЕНОМРЕЖОВ МОДЕЛИ НА DATA MINING ПРОЦЕСИ В СИГУРНОСТТА НА СИСТЕМИТЕ В ИНТЕЛИГЕНТЕН ДОМ.....	28
3.1 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА ПРОТИЧАНЕТО НА СЪСТОЯНИЯТА НА РЕАЛНИЯ РАЗПЛАЩАТЕЛЕН ПРОЦЕС В PGW.....	28
3.2 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА СТАНДАРТЕН ИНТЕРНЕТ ПОРТАЛ ЗА ЕЛЕКТРОННО РАЗПЛАЩАНЕ С ПОМОЩТА НА ИНТУИЦИОНИСТКИ РАЗМИТИ ОЦЕНКИ.....	32
3.3 ОБОБЩЕНОМРЕЖОВ МОДЕЛ ЗА ОЦЕНКА НА РИСКА ОТ КИБЕР- ВМЕШАТЕЛСТВО ВЪРХУ ДРОНОВЕ ЧРЕЗ ИЗПОЛЗВАНЕТО НА ИНТУИЦИОНИСТКИ РАЗМИТИ ОЦЕНКИ.....	36
3.4 МОДЕЛИРАНЕ НА ЗАХРАНВАЩАТА И ОХРАНИТЕЛНА СИСТЕМА НА SMART HOUSE.....	41
Приноси към дисертационния труд.....	49
Насоки за бъдещи изследвания.....	50
Публикации по дисертационния труд.....	51

Използвани съкращения/чуждоезикови обозначения

БЛУ	Безпилотно летателно устройство.
AI	Artificial Intelligence / изкуствен интелект.
Data Mining/DM	Извличане на данни.
Drone Radio Transmitter	Дрон, радио предавател.
FPV	First-person view flying \ Летене от първо лице.
FrSky, Spektrum, Futaba, Hitec, Devo, TBS	Известни производители на дронове.
GN IDE	Generalized Nets Integrated Development Environment \ Софтуерен инструмент за симулация на модели разработени с обобщени мрежи.
IFL	Intuitionistic Fuzzy Logic / Интуиционистка размита логика.
IFS	Intuitionistic Fuzzy Set / Интуиционистки размито множество.
LUA script	Програмен скрипт – с широко разпространение, често използван за програмирането на радио контролери за UAV.
Open TX	OpenTX е фърмуер с отворен код за RC радиопредаватели.
Payment Gateways	Портали за електронно разплащане
PGW	Payment Gateways / портал за електронно разплащане
RC	Radio Controller/Радио контролер.
RSSI	Received Signal Strength Indicator/ Индикация за силата на радиосигнала
Rx	Transmit/Изпращане на сигнал.
Smart	Интелигентно устройство.
Smart House	Интелигентен дом.
Throttle, Yaw, Pitch и Roll	Основни команди, необходими за управление на дрона.
Tx	Receive \ Получаване на сигнал.
UAV	Unmanned aerial vehicle\ Безпилотно летателно устройство.
И	Интелигентни системи.
OM	Обобщена мрежа.
Фърмуер	Базово програмно осигуряване.
ИД	Интелигентен дом
ИОТ	Интернет на нещата /Internet of Things/
DDoS	Отказ от обслужване
БД	База данни
IFE	Интуиционистка размита оценка /intuitionistic fuzzy estimation/
ПОС ТЕРМИНАЛ	Точка на покупко-продажба /point of sale/

БЛАГОДАРНОСТИ

На първо място искам да изразя благодарността си към моя научен ръководител проф. д-мн д-тн Красимир Атанасов за непрестанната подкрепа по време на докторантската ми изследователска дейност, за неговото търпение, мотивация, ентузиазъм и познание в областта. Неговите насоки, съвети и препоръки ми помагаша в периода на изследователската ми работа и писането на дисертационния труд. Моите благодарности са насочени също към колегите ми от катедра „Компютърни системи и технологии“ от Университет „Проф. д-р Асен Златаров“–гр. Бургас и специално към колегата ми Борис Бозвелиев, с когото съвместно разработвах част от научните си изследвания. Специални благодарности за вторият ми научен ръководител Проф. д-р Сотир Сотиров, за неговата непрестанна подкрепа по време на целия период на моето докторантско следване, както и за ценните насоки и опит, с който ми помагаше постоянно. И накрая, но не на последно място, бих искал да изразя моите благодарности към моето семейство, за непрестанната подкрепа към крайната цел, за тяхното разбиране и окуражаване и безрезервна вяра и подкрепа по всякакви възможни начини.

УВОД

Понятието „Интелигентен дом“ (ИД, Умен дом, Smart house) беше непознато за средностатистическия потребител до преди няколко години. Днес обаче се наблюдава богато разнообразие от атрактивни и полезни решения. Тяхната цел е да улеснят управлението, както и да осигурят безопасност и сигурност. Развитието в областта на автоматизацията, в комбинация с тенденциите, вдъхновени от „интернет на нещата (IoT – Internet of Things) даде на света концепцията за Умният дом (Smart Home). Идеята да се обединят всички устройства и системи в една хомогенна, високотехнологична платформа не е нова, но едва в последните години се наблюдават, макар и частични, но истенски работещи решения. Всички разработки и усилия обаче са насочени основно към управлението и контрола на елементите и системите в ИД – дистанционно включване или контролиране от приложения на компютър или смартфон. Така ИД наподобява детска количка с дистанционно управление. Все още липсват цялостните решения, които обединяват всички системи на ИД (осветителна, охранителна, информационна, градинска, гаражна, почистваща и т.н.) в един контролер, който да управлява системите по точно зададени от потребителя процеси. И нещо в повече – събиране и съхраняване на база от данни за потребителските навици, както и анализирането им, свързани с моментното (емоционално, физическо, времево и т.н.) състояние на потребителя. Липсва разработен модел, който автоматично да разпознава потребителя и да настройва системите в ИД според моментното му състояние на базата на натрупана информация във времето в базата от данни. От своя страна базата от данни трябва непрекъснато да се допълва и по този начин да се предоставя възможност за по-адаптивна реакция на контролера или устройството, управляващо ИД. Разбира се това е доста сложна задача, която изисква обобщаване и анализиране на изключително голям обем от данни, както и иновативен подход в описанието на съответните процесите, протичащи в ИД. Обобщените мрежи са най-подходящият начин за описание на тези процеси. Чрез създаване на обобщеномрежов модел ще могат да бъдат описани всички протичащи процеси в ИД, както и взаимовръзката между отделните компоненти на системата. Така могат да се синхронизират, наблюдават и обобщят процесите, взаимовръзките и контрола в ИД.

Друг важен въпрос е сигурността на умния дом. Доклад през 2016г. от NTT Data Corp. установи, че 80% от потребителите са загрижени за сигурността на споделените данни и комуникационни протоколи от умните устройства. Ако недоброжелател проникне в интелигентните устройства, би могъл да нанесе сериозни щети или да компрометира управлението им с цел нанасяне на вреди в ИД. От изключване на светлините и алармите, отключат вратите, като оставят дома незащитен, до включване на отоплителни и други такива уреди с цел злоумишлен палеж. Освен това недоброжелателите могат да имат потенциален достъп до мрежата, а оттам и да установят контрол над контролера на ИД. Могат да извършват системни наблюдения и вмешателства в личното пространство или източване на данни. През Октомври 2016 г. Mirai IoT ботнет, успя да свали част от интернет в серия от разпространени атаки срещу “отказ от обслужване” (DDoS), използвайки лошо защитени камери, DVR и рутери като входни точки. В допълнение към въпроса със сигурността, трябва да се отбележи притеснителният факт за поверителността на данните. Докладът за данни на NTT установи, че 73% от потребителите се притесняват за поверителността на данните, споделяни от техните домашни устройства.

Производителите на интелигентни устройства и платформи могат да събират данни за потребителите, с цел да подобрят продуктите си или да предлагат нови и подобрени услуги на клиентите. Доверието и прозрачността са от решаващо значение, но можем ли да разчитаме само на тях при изграждането и проектирането на системите на ИД? И тук възниква изключително важния въпрос за киберсигурността на системите в ИД. Освен развитието на управляващите системи (устройства, протоколи, БД и тн.) е необходимо реципрочно развитие и на системите за сигурност, които да осигурят безпроблемната работа на ИД, както и спокойствието на потребителите.

ЦЕЛ И ЗАДАЧИ НА ДИСЕРТАЦИОННИЯ ТРУД

Основната цел на настоящия дисертационен труд е да се изследват различни процеси от теорията на извличането на знания от данни (Data Mining) чрез моделирането им с помощта на обобщени мрежи и програмната реализация на основните от тях. За да бъде постигната тази цел, са поставени следните задачи:

1. Да се изследват и опишат процесите, протичащи в управлението на ИД чрез алгоритми за Data Mining процеси.
2. Да се разработят, опишат и представят някои от системите на ИД посредством Обобщени Мрежи (ОМ);
3. Да се разработи обобщеномрежов модел на система за сигурност чрез алгоритми за Data Mining процеси, като изследваме възможността за проникване и намеса в процесите на системата посредством разпита оценка чрез IFE.
4. Да се тества и представи една от системите в ИД чрез софтуера GN IDE.
5. Разработване на обобщеномрежов модел на разплащателна система.
6. Разработване на обобщеномрежов модел на захранващата и охранителна система на Smart house.
7. Да се опишат резултатите и да се направят съответните изводи.

1. ГЛАВА ПЪРВА - ОСНОВНИ ПОНЯТИЯ ОТ ТЕОРИЯТА НА ОБОБЩЕНИТЕ МРЕЖИ

Представени са основни понятия от теорията на обобщените мрежи

1.8 ИЗВОДИ

В Първа глава от дисертационния труд е направен обзор на същността на процеса на извличане на знания от данни и теорията на обобщените мрежи. Така се полага основата на разработването и анализа на обобщеномрежови модели, представени в следващите две глави на дисертационния труд.

Извличането на знания от данни е сложен и многоетапен процес. Различните етапи са събиране на данни, предварителна обработка и анализ. Фазата за предварителна обработка на данните е специфична за конкретните приложения, тъй като различните формати на данните изискват различни алгоритми да бъдат приложени към тях. Фазата на обработка може да включва, „изчистване“, интегриране на данни и извличане на характеристики. В някои случаи изборът на характеристики може да се използва и за по-точното представяне на данните. Някои градивни блокове, свързани с извличането на знания от данни често се използват многократно в различни приложни сценарии. Те съответстват на извличане на често срещани зависимости, клъстеризация, анализ на екстремалните стойности и класификация. Всички тези техники могат успешно да се моделират чрез обобщените мрежи.

От изложеното до тук става ясно, че обобщените мрежи могат да отразят логическите взаимовръзки във всеки моделиран чрез тях процес. Извлечената по време на процеса информация може да се съхранява посредством характеристиките на ядрата. Всички области на Изкуствения Интелект могат да се опишат чрез апарата на ОМ. Така могат да се създават много по-детайлни и по-общи модели на реални процеси. ОМ могат да бъдат математическо средство, което е в състояние да играе ролята на универсален език за описание на всякакви процеси в различни области. Това улеснява пренасянето на идеи от една област към друга, както и по-силна формализация и по-нататъшно развитие.

Към днешна дата може да се твърди, че извличането на данни е нова област в науката. DM може да се интерпретира като естествено разширение и обединение на някои от областите на ИИ.

В следващите две глави на дисертационния труд са представени нови разработени модели на алгоритми за Data Mining и клъстеризация, които допълват посочените по-горе в текста и спомагат за усилване на взаимовръзката между теорията на обобщените мрежи и извличането на знания от данни.

2. ГЛАВА ВТОРА - ОБОБЩЕНОМРЕЖОВИ МОДЕЛИ НА СИСТЕМИ ЗА DATA MINING ПРОЦЕСИ В ИНТЕЛИГЕНТЕН ДОМ

Направено е въведение на същността и структурата на интелигентния дом и влизане чрез разпознаване и определяне ниво на достъп

Представена е теоретична обосновка на обобщеномрежов модел на мрежа за автоматично включване и настройване на осветлението в помещение

2.1.2.1 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА АВТОМАТИЗИРАНА ОСВЕТИТЕЛНА СИСТЕМА В ПОМЕЩЕНИЕ.

Автоматизираните осветителни системи улесняват потребителите, особено тези в неравностойно положение, като им помагат чрез автоматично разпознаване да допуснат потребителя в помещението, както и да включат осветлението и различните уреди в помещенията. Тук ще разгледаме системата за автоматично включване на осветлението като опишем чрез обобщеномрежови модел процесите, протичащи при автоматичното разпознаване и настройване на осветителите.

Първоначално в обобщената мрежа влизат следните ядра:

α - Потребител - $i \in [1 \div n]$

β - База от данни

Υ - Идентификатор

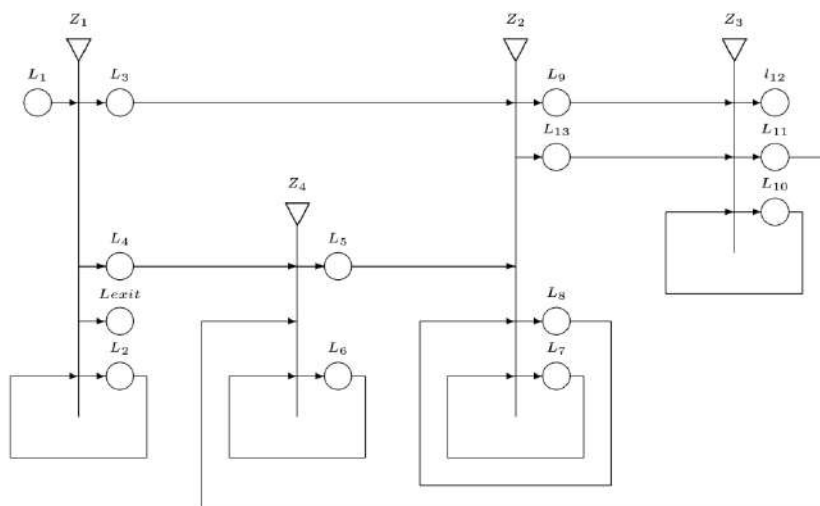
μ - Текущо състояние

Обобщеномрежовият модел на автоматизирана осветителна система (Фигура 2.1), реализиран чрез набор от преходи:

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

където преходите описват следния процес:

- Z_1 = „Разпознаване на ириса“;
- Z_2 = „Включване на осветлението в помещението“;
- Z_3 = „Въвеждане на корекции“;
- Z_4 = „Присвояване на параметрите за нивото на осветление“;



Фигура 2.1. Обобщенорежови модел на автоматизирана осветителна система.

$$Z_1 = \langle \{L_1, L_2\}, \{L_2, L_3, L_4, L_{exit}\}, R_1 \wedge (L_1, L_2) \rangle,$$

$$R_1 = \begin{array}{c|cccc} & L_2 & L_3 & L_4 & L_{EXIT} \\ \hline L_1 & True & False & False & False \\ L_2 & True & W_{2,3} & W_{2,4} & W_{2,exit} \end{array},$$

където:

$W_{2,3} = \text{“Ирисът е разпознат”}$

$W_{2,exit} = \neg W_{2,3}$

$W_{2,4} = W_{2,3}$

Ядрото β_1 постъпва на позиция L_2 , получава характеристиката „Данни за ириса в базата данни“.

Ядрото α_1 постъпва на позиция L_3 , получава характеристиката „Разпознат потребител“.

Ядрото Υ постъпва на позиция L_4 , получава характеристиката „Идентифициран ирис“.

Ядрото Υ_1 постъпва на позиция на L_{exit} , получава характеристиката „Неидентифициран ирис“.

$$Z_2 = \langle \{L_3, L_5, L_7, L_8\}, \{L_7, L_8, L_9, L_{13}\}, R_2 \wedge (L_3, L_5, L_7, L_8) \rangle,$$

$$R_2 = \begin{array}{c|cccc} & L_7 & L_8 & L_9 & L_{13} \\ \hline L_3 & False & False & True & False \\ L_5 & True & False & False & True \\ L_7 & True & True & False & True \\ L_8 & True & True & False & False \end{array},$$

Ядрото от L_5 се прехвърля към позиция L_{13} и не получава нови характеристики.

Ядрото от L_3 се прехвърля към позиция L_9 и не получава нови характеристики.

Ядрото α_1 , който постъпва на позиция L_3 , получава характеристиката „Разпознат потребител“.

Ядрото α_2 , който постъпва на позиция L_5 , получава характеристиката „Лични

настройки на потребителя за осветление и осветеност“.

Ядрото α_3 , който постъпва на позиция L_7 , получава характеристиката „Наличност на потребителя в помещението“.

Ядрото μ_1 , който постъпва на позиция L_8 , получава характеристиката „Гранична стойност“.

$$Z_3 = \langle \{ L_9, L_{13}, L_{10} \}, \{ L_{12}, L_{11}, L_{10} \}, R_3, \vee (L_{10}, \wedge (L_9, L_{13})) \rangle,$$

$$R_3 = \begin{array}{c|ccc} & L_{10} & L_{11} & L_{12} \\ \hline L_9 & False & False & True \\ L_{10} & True & W_{10,11} & False \\ L_{13} & True & True & False \end{array},$$

където:

$W_{10,11}$ = „Има корекции“.

Ядрото L_9 се прехвърля на позиция L_{12} и не получава нови характеристики.

Ядрото μ_2 , постъпва на позиция L_{10} и получава характеристика „Текущо състояние на настройките“.

Ядрото μ_3 , постъпва на позиция L_{11} и получава характеристиката „Корекции на личните опции на потребителя“.

$$Z_4 = \langle \{ L_4, L_6, L_{11} \}, \{ L_5, L_6 \}, R_4 \vee (L_4, L_6, L_{11}) \rangle,$$

$$R_4 = \begin{array}{c|cc} & L_5 & L_6 \\ \hline L_4 & False & True \\ L_6 & W_{6,5} & True \\ L_{11} & False & True \end{array},$$

където:

$W_{6,5}$ = Има намерени настройки за осветлението.

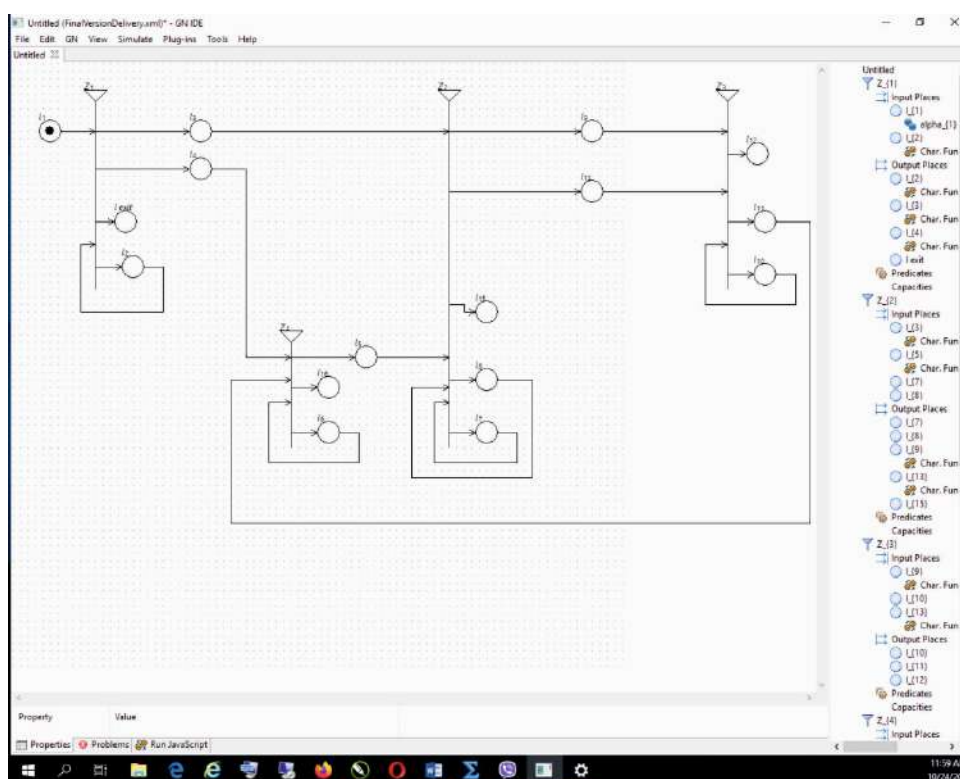
Ядрото β_2 , постъпва на позиция L_6 и получава характеристиката „База данни с лични опции за осветление“.

Ядрото γ , постъпва на позиция L_4 и получава характеристиката „Идентификатор на ирис“.

Системата за автоматично стартиране на осветлението се използва за улесняване на потребителя и особено на хората с увреждания. Той е в началото на процеса на интелигентния дом, като осигурява осветлението на помещението и помага за всички други следващи процеси. Моделът е представен със собствената си обобщена мрежа и показва процесите, през които потребителят преминава през системата, както и възникването на възможни грешки, които могат да бъдат причинени по един или друг начин. Обобщеномрежовият модел ни помага да анализираме възможните проблеми или да симулираме други проблеми, за да можем да оптимизираме поведението на системата.

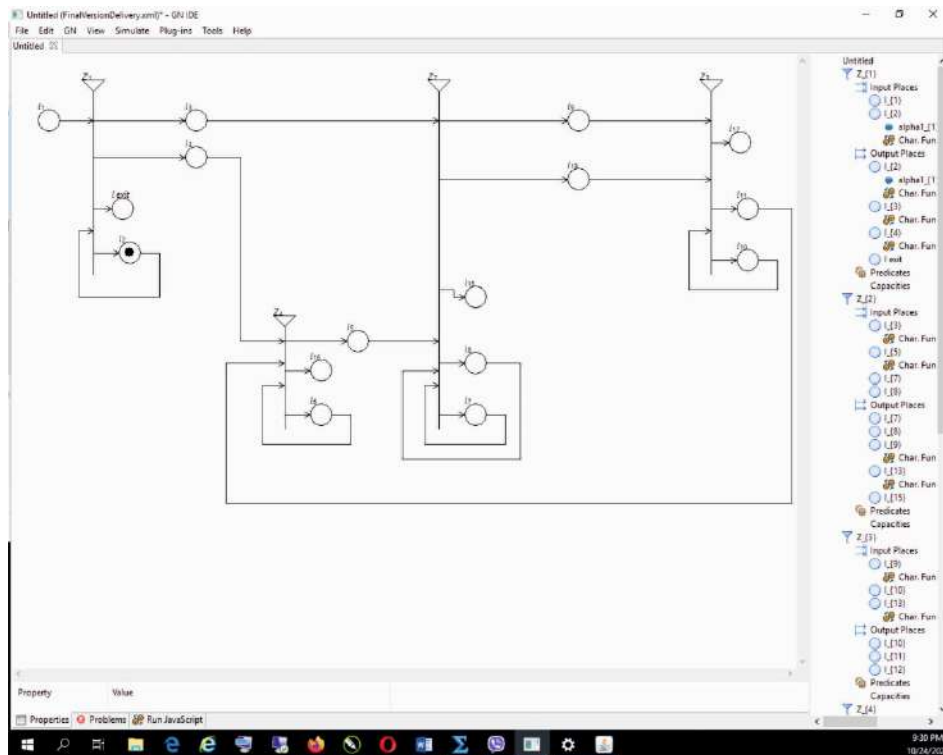
2.1.2.2 ДЕМОНСТРАТИВНА СИМУЛАЦИЯ НА ДЕЙСТВИЕТО НА АВТОМАТИЗИРАНА СИСТЕМА ЗА ОСВЕТЛЕНИЕ В GN IDE

Тук ще разгледаме демонстративната симулация в GN IDE, направена за да покаже действието на автоматизираната система за осветление, като са моделирани вероятности на база корекции върху данните на потребителя. Проследява се процесите от идентификацията на потребителя до включване или изключване на осветлението, като се минава през различните настройки и корекции. Софтуерът GN IDE е разработен специално за нуждите на симулацията на обобщеномрежовите модели, с цел ясна представа, наблюдение и анализ на процесите, които протичат през мрежата. При некоректно зададени данни или процеси, движението на ядрата от първоначалната към крайна точка на процесите прекъсва. Така се установяват некоректните данни или процеси и се предоставя възможност на разработчика за корекции.



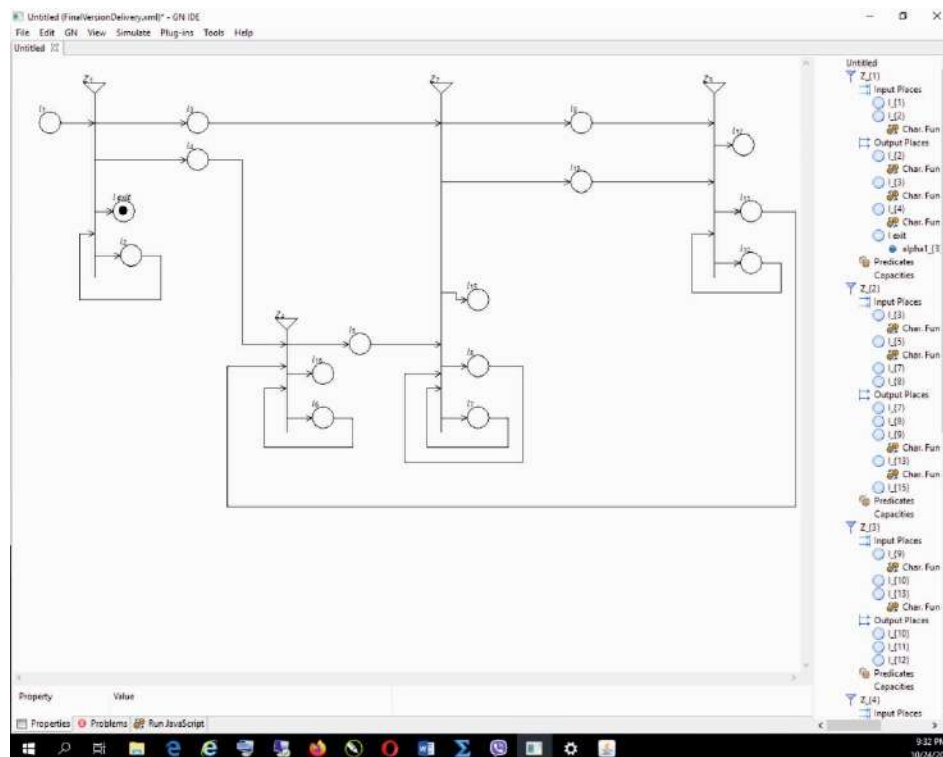
Фигура 2.2 Вход в системата.

Тук се вижда началото на процеса на идентификация и постъпването или отхвърлянето на потребителя в системата. Активно е ядрото L_1 , което е и началото на процеса.



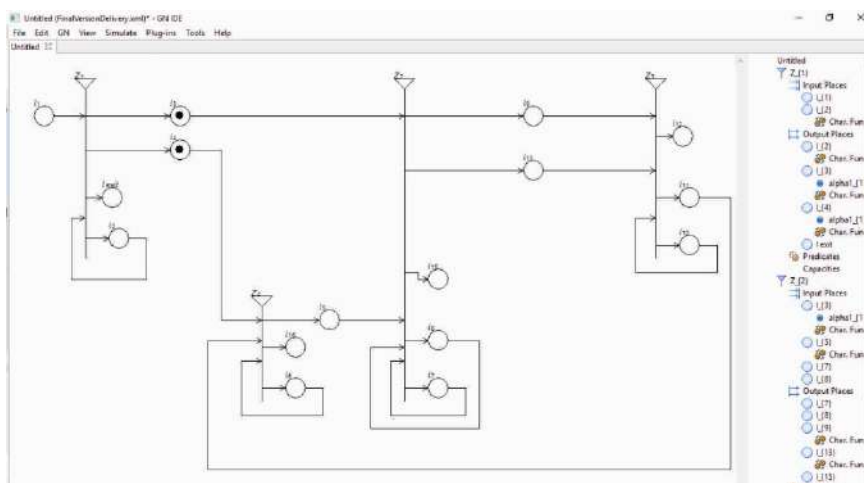
Фигура 2.3 Проверка в базата от данни на потребителите.

След като е постъпила заявка за вход в системата се извършва проверка в базата от данни на потребителите за наличието на такъв потребител, с цел допускане в системата или отхвърляне. При наличие на данни потребителят се допуска, съответно при отсъствие на данни потребителят се отхвърля, както е показано на фигура 2.4.



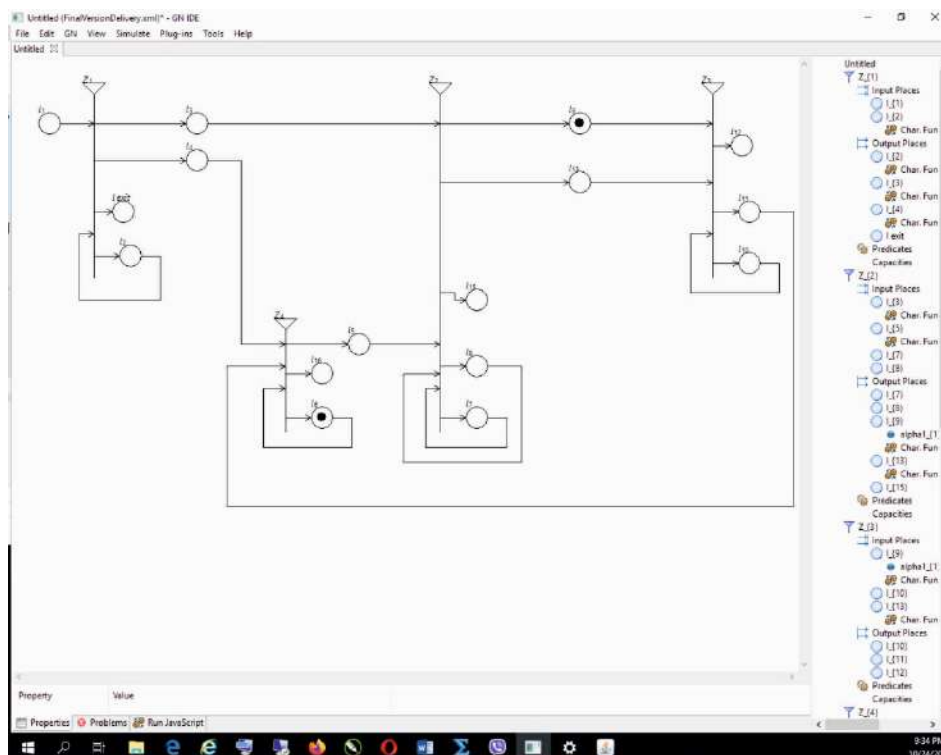
Фигура 2.4 Отхвърляне на заявката за вход.

При успешна верификация системата допуска потребителя да влезе като същевременно следи движението му и настройва системата да работи по неговите предварително зададени настройки и параметри, както е показано на фигура 2.5.

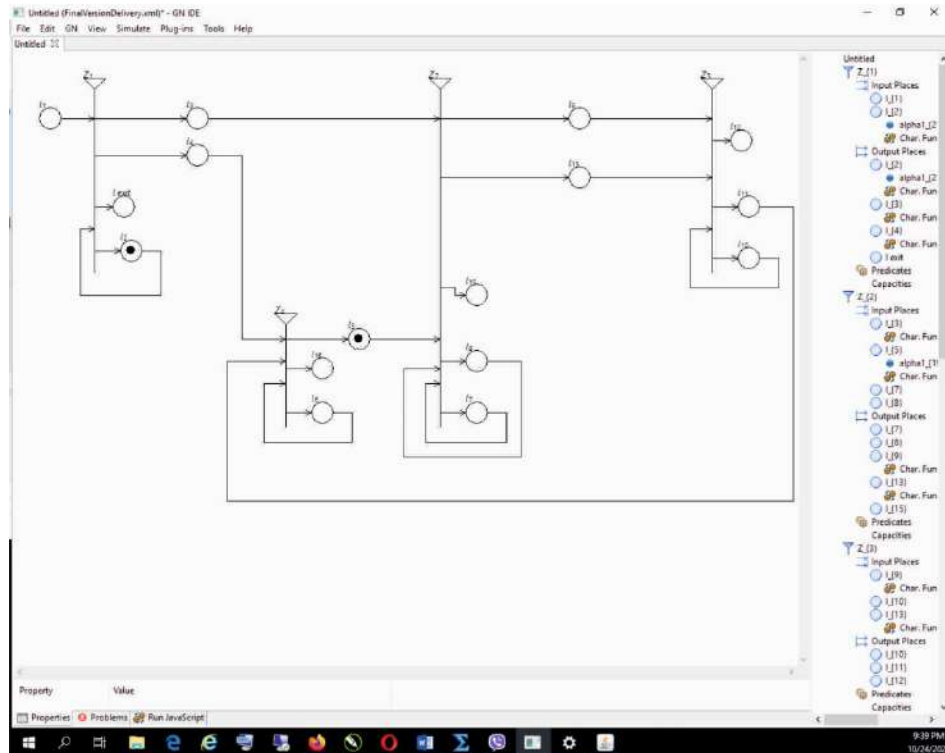


Фигура 2.5 Успешна верификация и придобиване на настройки на конкретния потребител.

Като следваща стъпка в процесите на системата е извличането от базата от данни на потребителските настройки. Тук системата избира въведените данни на потребителя и проследява движението му, както е показано на фигури 2.6 и 2.7.

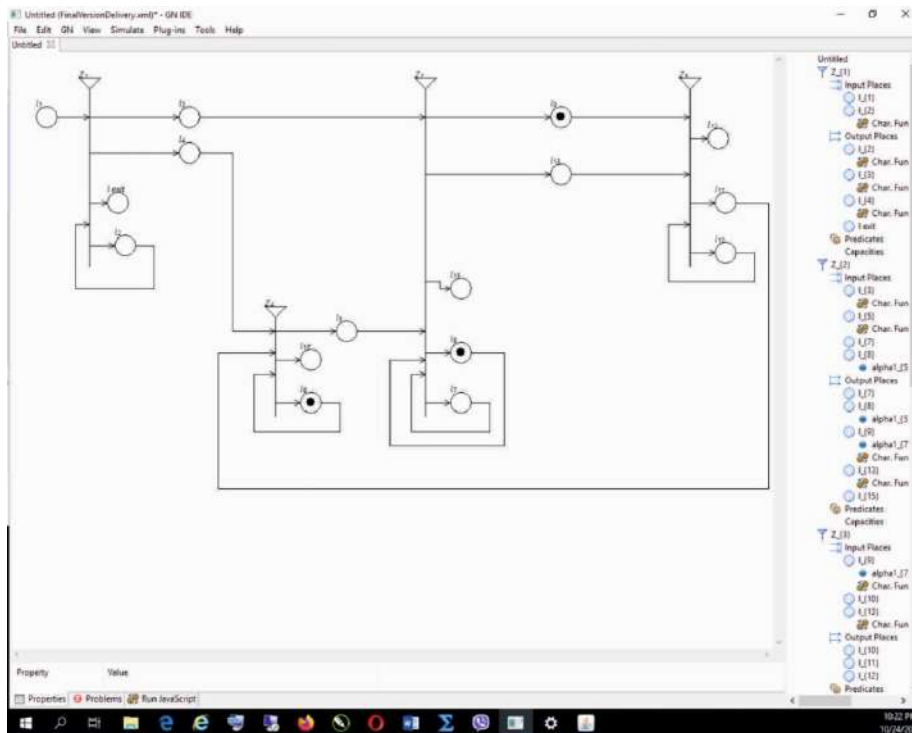


Фигура 2.6 Извличане на данни за потребителя.



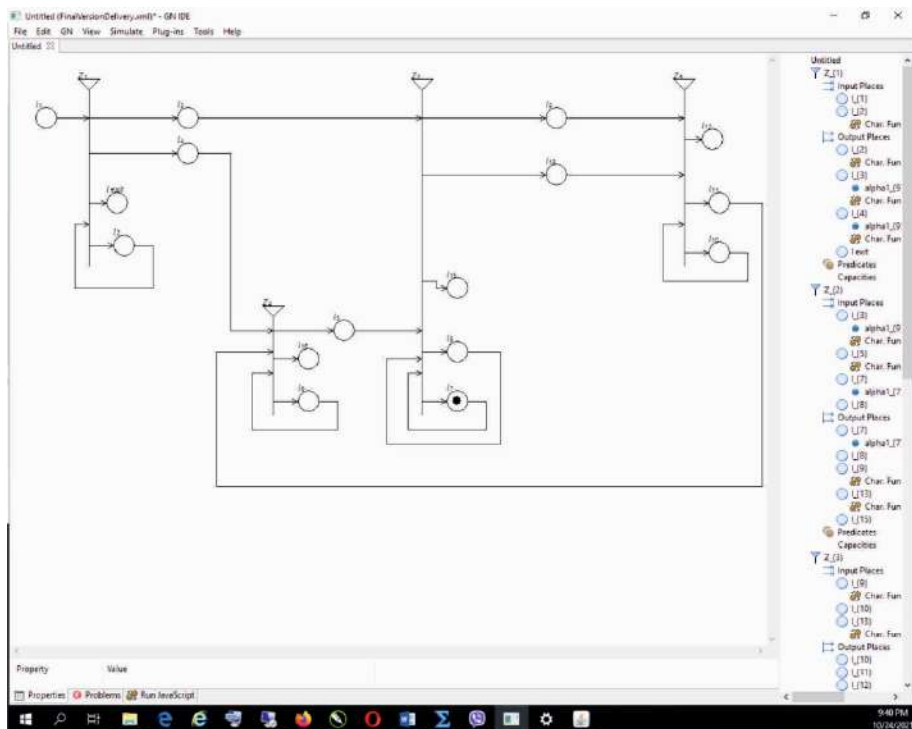
Фигура 2.7 Получаване на данни за настройки за потребителя.

Като следваща стъпка определяме проверката на проговата стойност за включване на осветлението. Тъй като осветлението е необходимо само когато осветеността в дадено помещение е по-малка от 150 Lux в системата има зададена стойност за минимален праг на осветеност. При стойности над тази прогова стойност осветението не се включва и не придобива настройките на потребителя поради липса на необходимост от него. При стойности на осветеността по-малки от 150 Lux осветлението се включва и придобива настройките на потребителя, като непрекъснато следи за наличието му в помещението. При установена липса на потребителя осветлението се изключва. Това е показано на фигури 2.8 и 2.9.



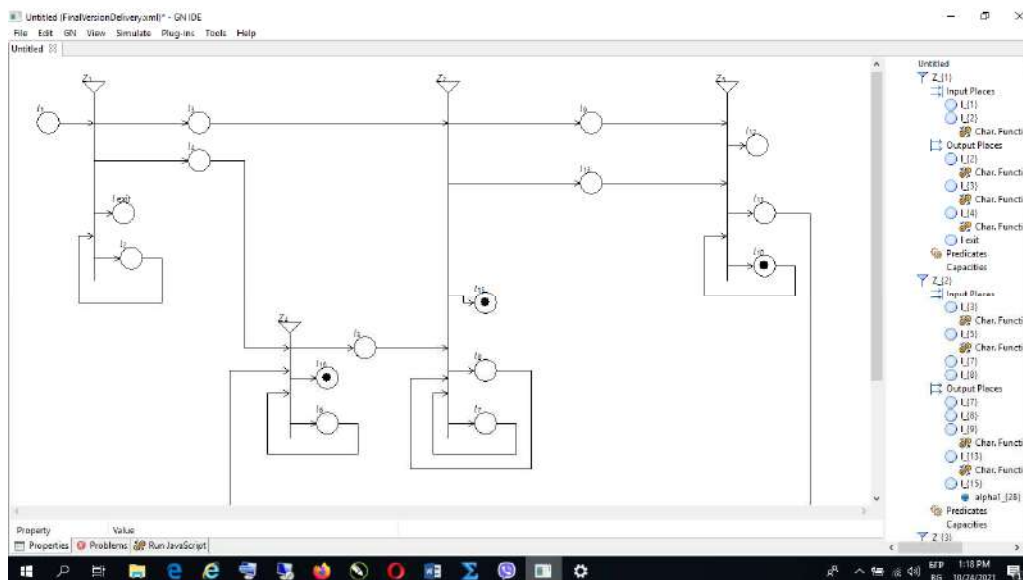
Фигура 2.8 Измерване на проговата стойност на осветеност.

Тук се проверява осветеността на помещението като се взимат данни и се сравняват в предварително зададената прагова стойност. Ако резултатът е по-нисък от зададения осветлението се включва като взема настройките (в случая ядрото L_6) и продължава нататък през ядрото L_9 , постъпвайки за настройките на необходима корекция, ако има такава. Процесът във фигура 9 е същия, но там се проверява чрез ядрото L_7 за наличие на потребител в помещението.

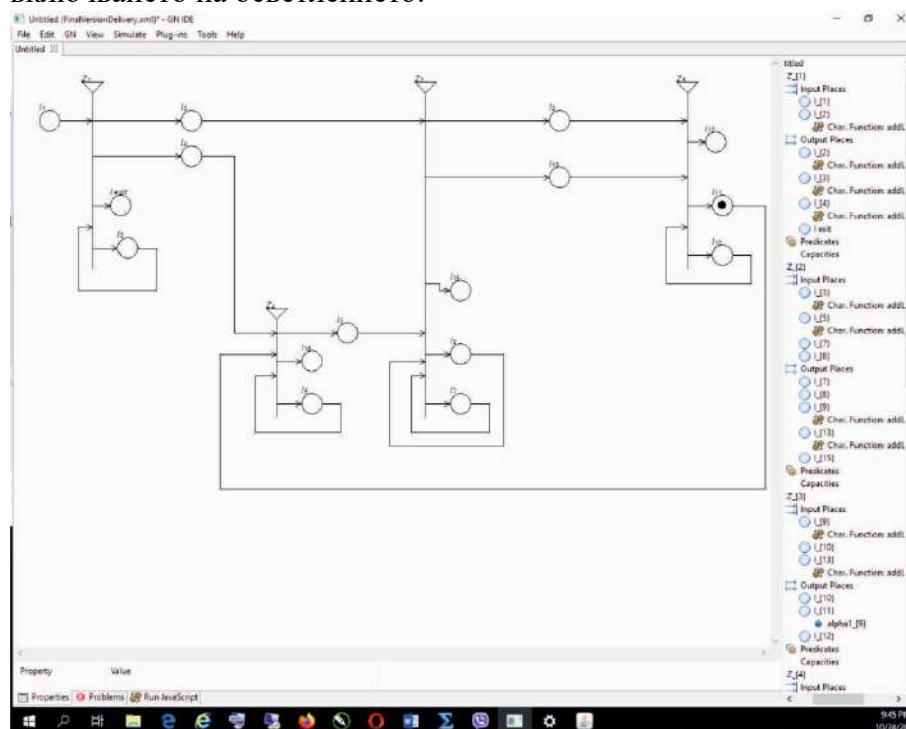


Фигура 2.. Проверка за наличието на потребител в помещението.

Във фигура 2.10 е показано липсата на потребител или наличие на осветеност над праговата стойност, в следствие на което няма нужда от придобиване на настройки за конкретния потребител в порцеса Z_4 , а в ядрата L_{16} и L_{15} процесът по включване и настройки на осветлението за конкретния потребител се прекратява.



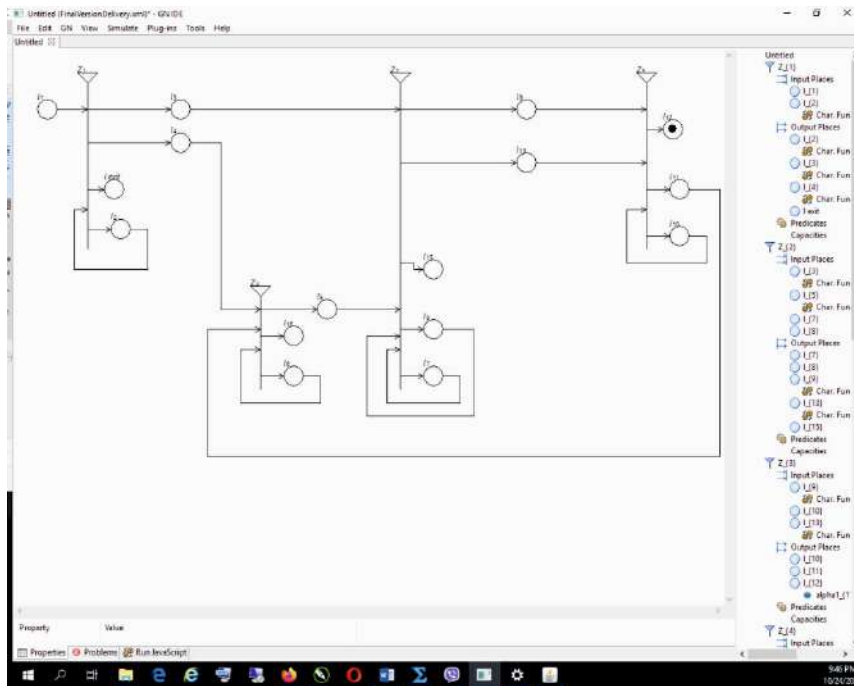
Фигура 2.10 Процес на прекратяване на придобиването на настройки и включването на осветлението.



Фигура 2.11 Нанасяне на корекции в базата от данни за настройките на потребителите.

На фигура 2.11 е показано необходимостта от нанасяне на корекции на осветлението, като потребителя нанася корекции в базата от данни.

В ядро L_{12} , на фигура 12 приключва целият цикъл от процеси, свързани с включването и настройките на осветлението на интелигентния дом.



Фигура 2.12 Завършване на процеса на настройките и корекциите.

2.2.1 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА КИБЕР СИСТЕМА ЗА ИНТЕЛИГЕНТЕН ДОМ С ИНТУИЦИОНИСТКА РАЗМИТА ОЦЕНКА

Представена е обща теория на IFS.

Ще разгледаме процеса чрез обобщеномрежови модел на Smart House [35, 42]. Обобщеномрежовият модел [7, 8] ще ни помогне лесно и ясно да разберем основния режим на работа на комуникациите в системите на Smart House. Ще ни покаже възможността за проникване, така че да сме в състояние да подобрим сигурността, да отстраним неизправности и по-добре да анализираме целия процес. В горния контекст ще направим оценка на възможностите за комуникационно проникване в системата на Smart House. Тук ще използваме интуиционистки размити множества (IFS). Интуиционистките размити множества [56, 71, 75, 77] представляват разширение на понятието за размити множества, както е определено от Zadeh [104], показващо функция $\mu_A(X)$, определяща членството на елемент x към множеството A , оценено в интервала $[0; 1]$. Разликата между размитите множества и интуиционистките размити множества (IFS) е в присъствието на втора функция $\nu_A(x)$, определяща нечленството на елемента x в множеството A , където $\mu_A(x) \in [0; 1] \quad \nu_A(x) \in [0; 1]$ при условие $\mu_A(x) + \nu_A(x) \in [0; 1]$.

Самият IFS официално се обозначава с :

$$A = \{ \langle x, \mu_A(x), \nu_A(x) \rangle \mid x \in E \} .$$

Нуждаем се (IFS), за да оценим евентуалното проникване в комуникацията. Оценка се представя посредством наредени двойки $\langle \mu, \nu \rangle$ на 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 е в позиции L₃, L₄, L₅, L₆, L₇, L₈, L₁₁, L₁₂, L₁₅.

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

където:

S - Всички опити за верификация.

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.

Нека да разгледаме обобщеномрежовия модел на кибер системата на Smart House.

За улеснение добавяме следните видове ядра:

Ω - Интуиционистка размита оценка

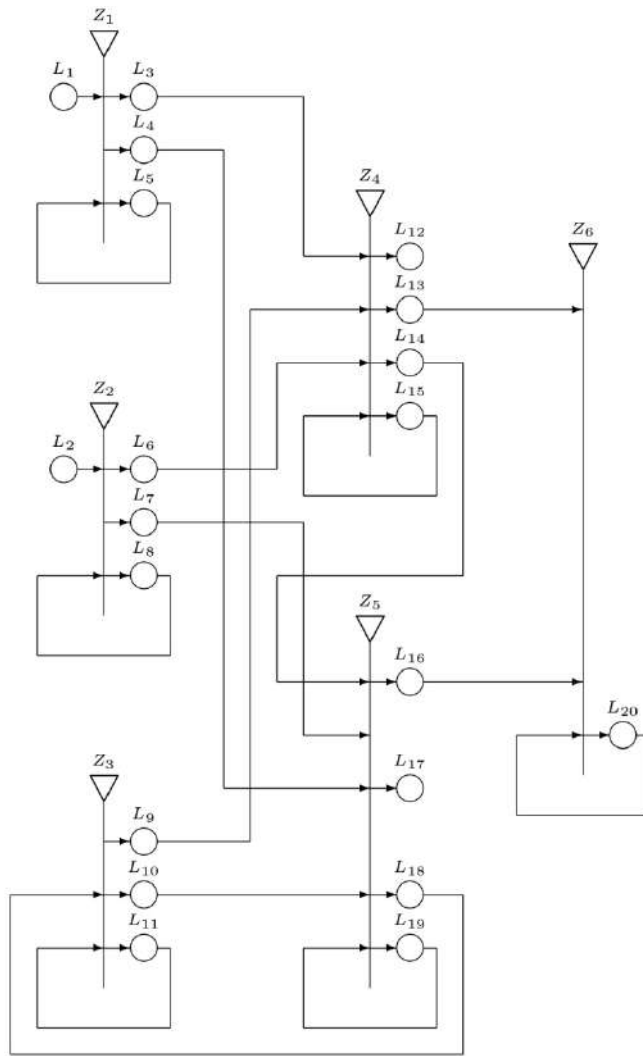
ω - Канали на протоколи, комуникации и управление.

Обобщеномрежовия модел на кибер системата на Smart House (Фигура 2.13) е реализирана чрез множество преходи:

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

Където се описва целия процес:

- Z₁ = „Действия на недоброжелателя“;
- Z₂ = „Действия на потребителя“;
- Z₃ = „Управление на процеси и протоколи“;
- Z₄ = „Процеси в облачната структура на платформата“;
- Z₅ = „Управление на системата“;
- Z₆ = „Интуиционистка размита оценка“;



Фигура 2.13 Обобщеномрежов модел на системите на Smart House.

$$Z_1 = \langle \{ L_1, L_5 \}, \{ L_3, L_4, L_5 \}, R_1, \wedge (L_1, L_5) \rangle,$$

$$R_1 = \begin{array}{c|ccc} & L_3 & L_4 & L_5 \\ \hline L_1 & False & False & True \\ \hline L_5 & W_{5,3} & W_{5,4} & False \end{array},$$

където:

$W_{5,3}$ = “ Недоброжелателят е пробил верификацията на облачната платформа ”

$W_{5,4}$ = “ Недоброжелателят е пробил верификацията на управлението на системите ”

Ядрото α постъпва на позиция L_1 и приема характеристика “Недоброжелател”.

Ядрото μ_1 постъпва на позиция L_3 и приема характеристика “Недоброжелателят разбива верификацията на облачната платформа”.

Ядрото μ_2 постъпва на позиция L_4 и приема характеристика “Недоброжелателят пробива верификацията на управлението на системите”.

Ядрото β_1 постъпва на позиция L_5 и приема характеристика

“База данни на нарушителя”.

$$Z_2 = \langle \{ L_2, L_8 \}, \{ L_6, L_7, L_8 \}, R_2, \vee (L_2, L_8) \rangle,$$

	L_6	L_7	L_8
L_2	<i>False</i>	<i>False</i>	<i>True</i>
L_8	$W_{8,6}$	$W_{8,7}$	<i>False</i>

където:

$W_{8,6}$ = “Проверката е коректна”

$W_{8,7}$ = “Недоброжелателят е пробил верификацията на базата от данни”

Ядрото Υ постъпва на позиция L_2 и приема характеристика “Потребител”.

Ядрото μ_3 постъпва на позиция L_6 и приема характеристика “Верификация за вход в облачната платформа”.

Ядрото μ_4 постъпва на позиция L_7 и приема характеристика “Верификация за вход в контролера на Smart House”.

Ядрото β_2 постъпва на позиция L_8 и приема характеристика “База данни на потребителя”.

$$Z_3 = \langle \{ L_{11}, L_{18} \}, \{ L_9, L_{10}, L_{11} \}, R_3, \vee (L_{11}, L_{18}) \rangle,$$

	L_9	L_{10}	L_{11}
L_{11}	$W_{11,9}$	$W_{11,10}$	<i>False</i>
L_{18}	<i>False</i>	<i>False</i>	<i>True</i>

където:

$W_{11,9}$ = “Верификацията е коректна”.

$W_{11,10}$ = “Верификацията е некоректна”.

Ядрото ω_1 постъпва на позиция L_9 и приема характеристика “Управление на интелигентно устройство”.

Ядрото ω_2 постъпва на позиция L_{10} и приема характеристика “Връзка с контролера на Smart House”.

Ядрото β_3 постъпва на позиция L_{11} и приема характеристика “База данни на протоколите”.

$$Z_4 = \langle \{ L_3, L_6, L_9, L_{15} \}, \{ L_{12}, L_{13}, L_{14}, L_{15} \}, R_4, \vee (L_{12}, L_{13}, L_{14}, L_{15}) \rangle,$$

	L_{12}	L_{13}	L_{14}	L_{15}
L_3	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_6	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_9	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_{15}	$W_{15,12}$	<i>True</i>	$W_{15,14}$	<i>False</i>

където:

$W_{15,14}$ = “Верификацията е коректна”.

$W_{15,12}$ = “Верификацията е некоректна”.

Ядрото Υ_2 постъпва на позиция L_{12} и приема характеристика “Exit”.

Ядрото Ω_1 постъпва на позиция L_{13} и приема характеристика “IFE идентификация”.

Ядрото ω_3 постъпва на позиция L_{14} и приема характеристика “Управление на

контролера ”.

Ядрото β_4 постъпва на позиция L_{14} приема характеристика “База данни на облачната платформа ”.

$$Z_5 = \langle \{ L_4, L_7, L_{10}, L_{14}, L_{19} \}, \{ L_{16}, L_{17}, L_{18}, L_{19} \}, R_5, \vee (L_4, L_7, L_{10}, L_{14}, L_{19}) \rangle,$$

$R_5 =$	L_{16}	L_{17}	L_{18}	L_{19}
L_4	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_7	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_{10}	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_{14}	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_{19}	$W_{19,16}$	$W_{19,17}$	$W_{19,18}$	<i>False</i>

където:

Ядрото Ω_2 постъпва на позиция L_{16} приема характеристика “IFE идентификация”.

Ядрото γ_3 постъпва на позиция L_{17} приема характеристика “Изход”.

Ядрото ω_4 постъпва на позиция L_{18} приема характеристика “Канали за комуникация на протоколите”.

Ядрото ω_5 постъпва на позиция L_{19} приема характеристика “Канали за реалните процеси, протичащи в системата”.

$$Z_6 = \langle \{ L_{13}, L_{16}, L_{20} \}, \{ L_{20} \}, R_6, \vee (L_{13}, L_{16}, L_{20}) \rangle,$$

$R_6 =$	L_{20}
L_{13}	<i>True</i>
L_{16}	<i>True</i>
L_{20}	<i>True</i>

където:

Ядрото Ω_3 постъпва на позиция L_{20} и приема характеристика “IFE Идентификация”.

От изложения по-горе анализ на системата "умна къща" става ясно, че за да се използва за улесняване на потребителя, процесите, протичащи в нея трябва да бъдат много добре защитени. В противен случай при намеса в който и да е канал на комуникация, недоброжелателят може да въздейства на системите по начин, неприемлив за потребителя, като по този начин има вероятност да нанесе непоправими щети, както на системите на Smart House, така и на самия потребител. Моделът се представя с обобщената му мрежа и показва процесите, които протичат в системата, както и възможните грешки, които могат да бъдат причинени. Разглежда се и възможността от проникване на недоброжелатели в системата с цел злонамереност, като се прилага размита оценка посредством интуиционистка размита оценка. Моделът на обобщена мрежа ни помага да анализираме възможните проблеми или да симулираме други проблеми, така че да можем да оптимизираме и предвидим поведението на системата.

2.2.2 АЛТЕРНАТИВЕН МЕТОД ЗА ОЦЕНКА НА РИСКА ОТ КИБЕР АТАКА НАД УПРАВЛЕНИЕТО НА SMART HOUSE ЧРЕЗ ИНТУИЦИОНИСТКА РАЦМИТА ОЦЕНКА

2.2.2.1 ОЦЕНКА НА РИСКА ОТ КИБЕРАТАКА НАД УПРАВЛЕНИЕТО НА SMART HOUSE ЧРЕЗ IFE

Тук ще добавим още четири степени на възможностите за проникване в системата на Умната къща, като оценките ще бъдат разделени на: Силно оптимистична, оптимистична, песимистична и силно песимистична. Тук разглеждаме обобщеномрежов модел на Smart House [3*, 7*]. По този начин ще допълним и продължим по-горе разгледаните сценарии за проникване в системите на Smart House, както и да разширим оценките за проникване в киберсистема за интелигентен дом с интуиционистки размити оценки [8*]. Обобщеномрежовият модел ще ни помогне лесно и ясно да разберем основния начин на комуникация на системите в Smart House и възможността за проникване, така че да можем да подобрим сигурността, отстраняването на неизправности и да анализираме по-добре целия процес. В горния контекст ще оценим възможностите за проникване на комуникация в системата на интелигентната къща чрез гореспоменатите оценки. Тук ще използваме интуиционистки размити множества.

Строго оптимистична формула:

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

Оптимистична формула:

$$\langle \mu, \nu \rangle = \langle \max(\mu_1, \mu_2, \dots, \mu_k), \min(\nu_1, \nu_2, \dots, \nu_k) \rangle$$

Песимистична формула:

$$\langle \mu, \nu \rangle = \langle \min(\mu_1, \mu_2, \dots, \mu_k), \max(\nu_1, \nu_2, \dots, \nu_k) \rangle$$

Строго песимистична формула:

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

2.2.2.2 ОБОБЩЕНОМРЕЖОВ МОДЕЛ ЗА ОЦЕНКА НА ВЪЗМОЖНОСТТА ЗА ПРОНИКВАНЕ В СИСТЕМИТЕ НА SMART HOUSE ЧРЕЗ IFE.

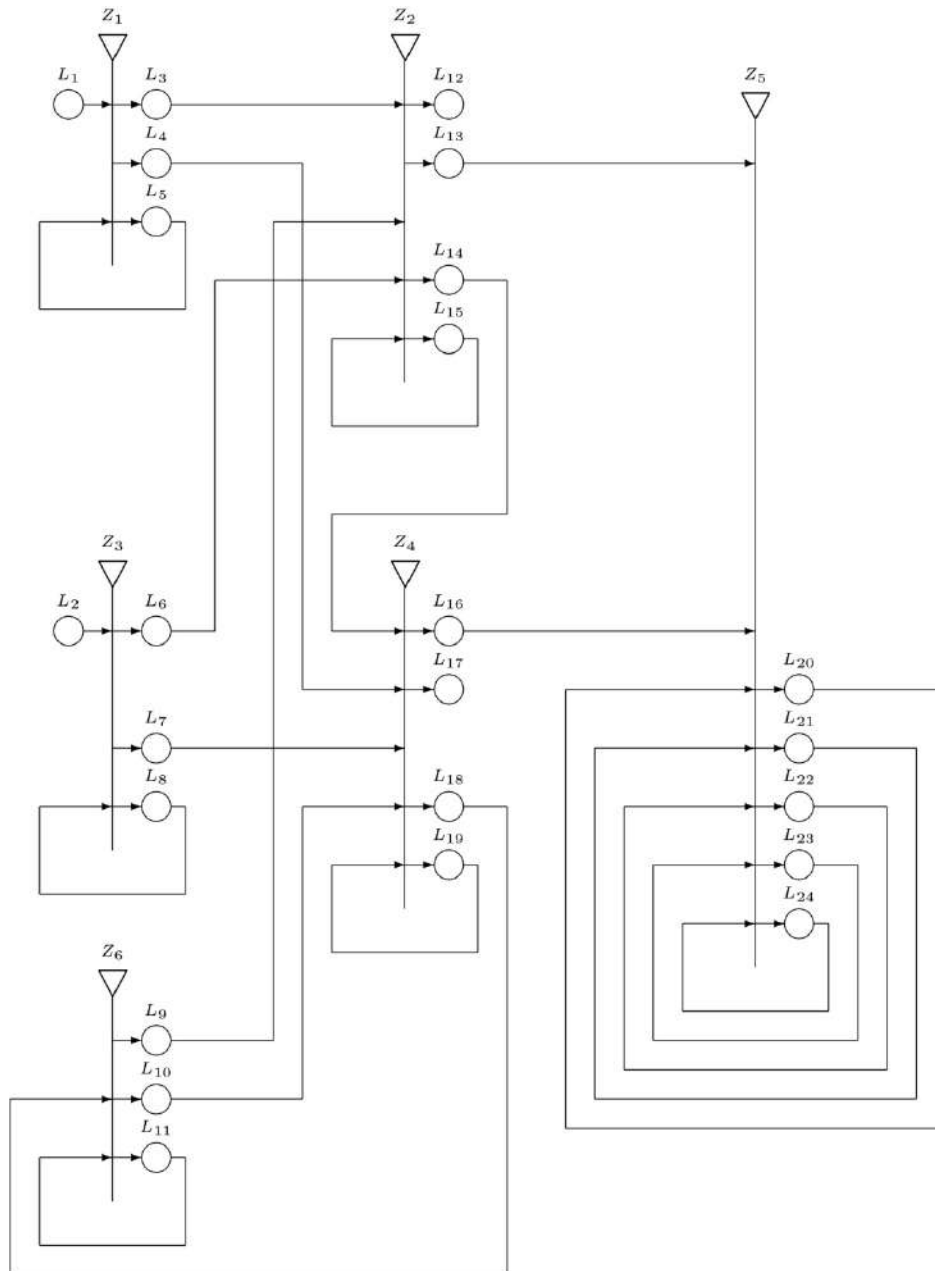
Системата на Smart House улеснява потребителите. Първоначално в обобщената мрежа влизат вече дефинираните по-горе ядра: $\alpha, \beta, \gamma, \mu, \Omega, \omega$.

Обобщеномрежовият модел на системите на Smart House (Фигура 2.14) е представен чрез набор от преходи:

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

където преходите описват следните процеси:

- Z_1 = „Действия на нарушителя“;
- Z_2 = „Управление на облачната платформа“;
- Z_3 = „Действия на потребителя“;
- Z_4 = „Управление на системите“;
- Z_5 = „IFE Оценка“;
- Z_6 = „Управление на протоколите за комуникация“;



Фигура 2.14 Обобщеномрежов модел на системите на Smart House.

$$Z_1 = \langle \{ L_1, L_5 \}, \{ L_3, L_4, L_5 \}, R_1, \wedge (L_1, L_5) \rangle,$$

$$R_1 = \begin{array}{c|ccc} & L_3 & L_4 & L_5 \\ \hline L_1 & False & False & True \\ L_5 & W_{5,3} & W_{5,4} & False \end{array},$$

където:

$W_{5,3}$ = “Недоброжелателят успява да пробие верификацията на облачната платформа”

$W_{5,4}$ = “Недоброжелателят успява да пробие верификацията на управлението на системите”

Ядрото α постъпва на позиция L_1 и приема характеристика “Недоброжелател”.

Ядрото γ_1 постъпва на позиция L_3 и приема характеристика

“Недоброжелателят пробива верификацията на облачната платформа”.
 Ядрото γ_2 постъпва на позиция L_4 и приема характеристика
 “Недоброжелателят пробива верификацията на управлението на системите”.

Ядрото β_1 постъпва на позиция L_5 и приема характеристика “База от данни на недоброжелателя”.

$$Z_2 = \langle \{ L_3, L_6, L_9, L_{15} \}, \{ L_{12}, L_{13}, L_{14}, L_{15} \}, R_2, \vee (L_{12}, L_{13}, L_{14}, L_{15}) \rangle ,$$

	L_{12}	L_{13}	L_{14}	L_{15}
L_3	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_6	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_9	<i>False</i>	<i>False</i>	<i>False</i>	<i>True</i>
L_{15}	$W_{15,12}$	<i>True</i>	$W_{15,14}$	<i>False</i>

където:

$W_{15,14}$ = “Верификацията е коректна”.

$W_{15,12}$ = “Верификацията не е коректна”.

Ядрото μ_2 постъпва на позиция L_{12} и приема характеристика
 “Изход”.

Ядрото ω_1 постъпва на позиция L_{13} и приема характеристика
 “IFE идентификатор”.

Ядрото Ω_3 постъпва на позиция L_{14} и приема характеристика
 “Управление на контролера”.

Ядрото β_4 постъпва на позиция L_{14} и приема характеристика
 “База от данни на облачната платформа”.

$$Z_3 = \langle \{ L_2, L_8 \}, \{ L_6, L_7, L_8 \}, R_3, \vee (L_2, L_8) \rangle ,$$

	L_6	L_7	L_8
L_2	<i>False</i>	<i>False</i>	<i>True</i>
L_8	$W_{8,6}$	$W_{8,7}$	<i>False</i>

Където:

$W_{8,6}$ = “Верификацията е коректна”

$W_{8,7}$ = “Недоброжелателят е пробил верификацията на достъпа до базата от данни”.

Ядрото μ постъпва на позиция L_2 и приема характеристика
 “Потребител”.

Ядрото γ_3 постъпва на позиция L_6 и приема характеристика
 “Верификация за вход в облачната платформа”.

Ядрото γ_4 постъпва на позиция L_7 и приема характеристика
 “Верификация за вход в контролера на Smart House”.

Ядрото β_2 постъпва на позиция L_8 и приема характеристика
 “База данни на потребителя”.

$$Z_4 = \langle \{ L_4, L_7, L_{10}, L_{14}, L_{19} \}, \{ L_{16}, L_{17}, L_{18}, L_{19} \}, R_4, \vee (L_4, L_7, L_{10}, L_{14}, L_{19}) \rangle ,$$

$$R_4 = \begin{array}{c|cccc} & L_{16} & L_{17} & L_{18} & L_{19} \\ \hline L_4 & False & False & False & True \\ L_7 & False & False & False & True \\ L_{10} & False & False & False & True \\ L_{14} & False & False & False & True \\ L_{19} & W_{19,16} & W_{19,17} & W_{19,18} & False \end{array},$$

Ядрото ω_2 постъпва на позиция L_{16} и приема характеристика “Идентификация на IFE”.

Ядрото μ_3 постъпва на позиция L_{17} и приема характеристика “Изход”.

Ядрото Ω_4 постъпва на позиция L_{18} и приема характеристика “Каналите за протоколи”.

Ядрото Ω_5 постъпва на позиция L_{19} и приема характеристика “Канали на реалните процеси, протичащи в системата”.

$$Z_5 = \langle \{ L_{13}, L_{16}, L_{20}, L_{21}, L_{22}, L_{23}, L_{24} \}, \{ L_{20}, L_{21}, L_{22}, L_{23}, L_{24} \}, R_5, \vee (L_{13}, L_{16}, L_{20}, L_{21}, L_{22}, L_{23}, L_{24}) \rangle,$$

$$R_5 = \begin{array}{c|ccccc} & L_{20} & L_{21} & L_{22} & L_{23} & L_{24} \\ \hline L_{13} & True & True & True & True & True \\ L_{16} & True & True & True & True & True \\ L_{20} & True & False & False & False & False \\ L_{21} & False & True & False & False & False \\ L_{22} & False & False & True & False & False \\ L_{23} & False & False & False & True & False \\ L_{24} & False & False & False & False & True \end{array},$$

Ядрото ω_3 постъпва на позиция L_{20} и приема характеристика “Идентификация на IFE”.

Ядрото ω_4 постъпва на позиция L_{21} и приема характеристика “Строго оптимистична Идентификация на IFE”.

Ядрото ω_5 постъпва на позиция L_{22} и приема характеристика “Оптимистична Идентификация на IFE”.

Ядрото ω_6 постъпва на позиция L_{23} и приема характеристика “Песимистична Идентификация на IFE”.

Ядрото ω_7 постъпва на позиция L_{24} и приема характеристика “Строго песимистична Идентификация на IFE”.

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

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

където:

$W_{11,9}$ = “Верификацията е коректна”.

$W_{11,10}$ = “Верификацията е некоректна”.

Ядрото Ω_1 постъпва на позиция L_9 и приема характеристика
“Управление на умните устройства”.

Ядрото Ω_2 постъпва на позиция L_{10} и приема характеристика
“Връзка с контролера на Smart House”.

Ядрото β_3 постъпва на позиция L_{11} и приема характеристика
“База от данни на протоколите и каналите за комуникация”.

От изложеното по-горе се вижда ясно, че посредством интуиционистките размити оценки може да се направи изключително подробен и точен анализ, както и да се направи оценка на опитите за пробиване на кибер сигурността на системите, а също така и за входовете на оторизираните потребители и техните грешки при опитите им за достъп в системите, протоколите и облачната платформа на Smart House. Системата „интелигентен дом“ се използва за улесняване на потребителя. Моделът е представен с неговата обобщена мрежа и показва процесите, които протичат в системата, както и възможните грешки, които могат да бъдат причинени. Разглежда се и възможността за злонамерено влизане в системата, като се използват размити степени чрез интуиционистки размити оценки. Моделът GN ни помага да анализираме възможни проблеми или да симулираме други проблеми, за да можем да оптимизираме поведението на системата. Различните видове интуиционистки размити оценки могат да служат като основа за по-нататъшен анализ и предвиждане с цел предотвратяване на различни типове опити за проникване в системите на Smart House.

2.3 ИЗВОД

В Глава втора от дисертационния труд с помощта на апарата на обобщените мрежи са разработени модели на процеси, свързани с извличане на знания от данни. По този начин можем да анализираме отделните стъпки и да се вникне по-дълбоко в начина им на действие.

Анализът изисква разпределеното извличане на потоци от данни да се извършва в реално време. Предизвикателствата на алгоритмите за извличане на големи данни са: локално обучение и сливане на данни за множество източници на информация; извличане на знания от оскъдни, несигурни и непълни данни; извличане на знания от сложни и динамични данни.

Обобщеномрежовият модел на автоматизираната осветителна система може да бъде използван за изследване и наблюдение. Също така, той може да се допълни със споменатите в началото на настоящата глава разширения към процеса. В допълнение, в GN IDE е направена демонстрация на действието на автоматизираната система за осветление, като са моделирани вероятности на база корекции върху данните на потребителя.

Обобщеномрежовият модел на кибер системата на интелигентния дом, представен в настоящото изследване, разделя процеса на верификация на двете му основни страни – одобрена верификация и отхвърлена верификация и ги описва в детайли, което от своя страна способства за по-задълбочено вникване в начина на действие на процеса и алгоритъма. Чрез интуиционистка размита оценка направихме анализ за възможните начини на проникване през защитата и намесване в дейността на системата. Представени са и различни възможности на кибер заплахи в такава среда.

3. ГЛАВА ТРЕТА - ОБОБЩЕНОМРЕЖОВ МОДЕЛИ НА DATA MINING ПРОЦЕСИ В СИГУРНОСТТА НА СИСТЕМИТЕ В ИНТЕЛИГЕНТЕН ДОМ

Представена е обща теория за data mining процеси в сигурността на системите в интелигентен дом

3.1 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА ПРОТИЧАНЕТО НА СЪСТОЯНИЯТА НА РЕАЛНИЯ РАЗПЛАЩАТЕЛЕН ПРОЦЕС В PGW

Представена е теория за реалния разплащателен процес в pgw

Обобщеномрежови модел на електронно разплащане (Фиг. 3.1). Той съдържа множество 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:

$$Z_{1,1} = \langle L_u, L_{3,x} \rangle \{ L_{1,1}, L_{1,x}, L_{3,x}, L_{5,x} \}, R_{1,1}, \vee (L_u, L_{3,x}),$$

	$L_{1,1}$	$L_{1,x}$	$L_{3,x}$	$L_{5,x}$	
$R_{1,1} =$	Lu	false	false	true	false
	$L_{3,x}$	$W_{3,x,1,1}$	$W_{3,x,1,x}$	true	$W_{3,x,5,x}$

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 “;

Ядрото което влиза в позиция L_u получава характеристика “Потребител”.

Ядрото което влиза в позиция $L_{3,x}$ получава характеристика “Първа банка проверка на БД” .

Ядрото което влиза в позиция $L_{1,1}$ получава характеристика “Първа банка успешна проверка”.

Ядрото което влиза в позиция $L_{1,x}$ получава характеристика “Проверка на банка “X” ”.

Ядрото което влиза в позиция $L_{5,x}$ получава характеристика “Банковата проверка е неуспешна”.

$$Z_{1,x} = \langle \{ L_{1,x} \} \{ L_{4,x} \}, R_{1,x}, \vee (L_{1,x}), \rangle,$$

където:

$$R_{1,x} = \frac{L_{4,x}}{L_{1,x} \mid true}$$

Ядрото, което влиза в позиция $L_{1,x}$, получава характеристиката „Проверка на кредитна карта от първата банка“.

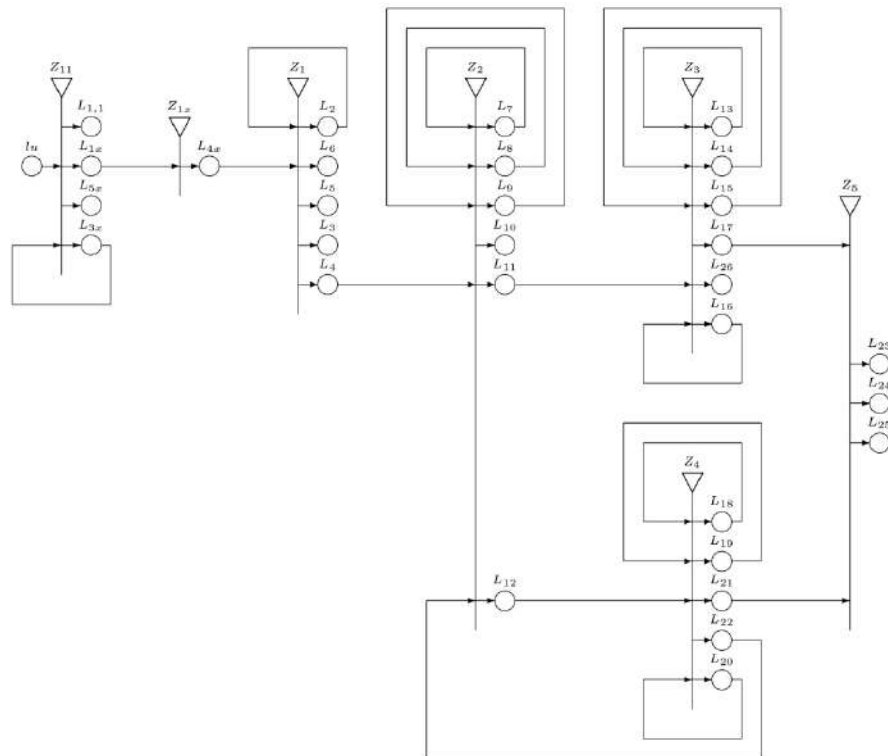
Ядрото, което влиза в позиция $L_{4,x}$, получава характеристиката „Проверка на кредитната карта от X -тата банка“.

Ядрото, което влиза позиция $L_{1,x}$ получава характеристиката “Валидиране на кредитната карта от първата банка”.

Ядрото, което влиза позиция $L_{4,x}$ получава характеристиката “Валидиране на кредитната карта от X -тата банка”.

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

R_1	L_2	L_3	L_4	L_5	L_6
$L_{1,1}$	true	$W_{1,1,3}$	false	$W_{1,1,5}$	$W_{1,1,6}$
$L_{4,x}$	true	$W_{4,x,3}$	false	$W_{4,x,5}$	$W_{4,x,6}$
L_2	true	$W_{2,3}$	$W_{2,4}$	$W_{2,5}$	$W_{2,6}$



Фиг. 3.1 Обобщеномрежови модел на реален разплащателен процес в PGW където:

$W_{1,1,3}$ = „Наличността по картата от първата банка е ≤ 0 “;

$W_{1,1,5}$ = „Има направен отказ на потребителя от заявката“;

$W_{1,1,6}$ = „Потребителят не е заявил опит за плащане“;

$W_{4,x,3}$ = „Наличността по картата от ‘X-тата банка е ≤ 0 “;

$W_{4,x,5}$ = „Прекъсната е заявка от потребител“;

$W_{4,x,6}$ = „Не е заявен опит за плащане от потребителя“; $W_{2,3} = W_{1,3}$ “;

$W_{2,4} = \neg W_{1,3}$ “;

$W_{2,6} = \neg W_{1,6}$;

Ядрото, което влиза в позиция $L_{1,x}$ получава характеристика
“Проверка на кредитна карта от първата банка”.

Ядрото, което влиза в позиция $L_{4,x}$ получава характеристика
“Проверка на кредитната карта от X -тата банка”.

Ядрото, което влиза в позиция L_2 получава характеристика
“Наличност по карта”.

Ядрото, което влиза в позиция L_3 получава характеристика
“Статус отказан”.

Ядрото, което влиза в позиция L_4 получава характеристика
“Приета потребителска карта”.

Ядрото, което влиза в позиция L_5 получава характеристика
“Статус отменен”.

Ядрото, което влиза в позиция L_6 получава характеристика “Статус изоставен”.

$Z_2 = \langle \{L_7, L_8, L_9, L_4, L_{22}\} \{L_7, L_8, L_9, L_{10}, L_{11}, L_{12}\}, R_2, \vee (L_4, L_7, L_8, L_9, L_{22}) \rangle$,

$R_2 =$	L_7	L_8	L_9	L_{10}	L_{11}	L_{12}
L_7	<i>true</i>	$W_{7,8}$	<i>false</i>	$W_{7,10}$	<i>false</i>	<i>false</i>
L_8	<i>false</i>	<i>true</i>	<i>true</i>	$W_{8,10}$	<i>false</i>	<i>false</i>
L_9	<i>false</i>	<i>false</i>	<i>true</i>	$W_{9,10}$	$W_{9,11}$	$W_{9,12}$
L_4	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>
L_{22}	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>

където:

$W_{7,8}$ = Има потвърждение на разплащателния портал, за успешно плащане” ;

$W_{7,10}$ = “ Съществува роблем със заявката ” ;

$W_{8,10}$ = “ $W_{7,10}$ ” ;

$W_{9,10}$ = “ $W_{7,10}$ ” ;

$W_{9,11}$ = “ Избрано е ръчно подаване на критериен алгоритъм” ;

$W_{9,12}$ = \neg “ $W_{9,11}$ ” ;

Ядрото, което влиза в позиция L_7 получава характеристика
“Статус – състояние на изчакване”.

Ядрото, което влиза в позиция L_8 получава характеристика
“Метод на плащане”.

Ядрото, което влиза в позиция L_9 получава характеристика
“Критерий алгоритъм за обработка на плащанията”.

Ядрото, което влиза в позиция L_{10} получава характеристика
“Статус отказан”.

Ядрото, което влиза в позиция L_{11} получава характеристика
“Потребителят завърши статус ръчен”.

Ядрото, което влиза в позиция L_{12} получава характеристика
“Потребителят завърши статус автоматичен”.

$Z_3 = \langle \{L_{13}, L_{14}, L_{15}, L_{16}, L_{11}\} \{L_{13}, L_{14}, L_{15}, L_{16}, L_{17}, L_{26}\}, R_3, \vee (L_{13}, L_{14}, L_{15}, L_{16}, L_{11}) \rangle$,

$$R_3 = \begin{array}{c|cccccc} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_{26} \\ \hline L_{13} & true & true & false & false & false & W_{13,26} \\ L_{14} & false & true & true & false & false & W_{14,26} \\ L_{15} & false & false & true & true & false & W_{15,26} \\ L_{16} & false & false & false & true & W_{16,17} & W_{16,26} \\ L_{11} & true & false & false & false & false & false \end{array},$$

където:

$W_{13,26} =$ „Има ръчна смяна от администратора на статус “отказан” ;

$W_{14,26} =$ „ $W_{13,26}$ “;

$W_{15,26} =$ „ $W_{13,26}$ “;

$W_{16,17} = \neg$ „ $W_{13,26}$ “;

$W_{16,26} =$ „ $W_{13,26}$ “;

Ядрото, което влиза в позиция L_{13} получава характеристика “Ръчен режим на плащане”.

Ядрото, което влиза в позиция L_{14} получава характеристика “Статус плащането изпратено”.

Ядрото, което влиза в позиция L_{15} получава характеристика “Статус чакащо плащане”.

Ядрото, което влиза в позиция L_{16} получава характеристика “Ръчно изпращане на администраторът”.

Ядрото, което влиза в позиция L_{17} получава характеристика “Успешна потребителска транзакция”.

Ядрото, което влиза в позиция L_{26} получава характеристика “Статус отхвърлен от администратор”.

$$Z_4 = \langle \{ L_{18}, L_{19}, L_{20}, L_{12} \} \{ L_{17}, L_{18}, L_{19}, L_{20}, L_{21} \}, R_4, \vee (L_{18}, L_{19}, L_{20}, L_{12}) \rangle,$$

$$R_4 = \begin{array}{c|ccccc} & L_{18} & L_{19} & L_{20} & L_{21} & L_{22} \\ \hline L_{12} & true & false & false & false & false \\ L_{18} & true & true & false & false & false \\ L_{19} & false & true & true & false & false \\ L_{20} & false & false & true & W_{20,21} & W_{20,22} \end{array},$$

където:

$W_{20,22} =$ „Има поне 5 неуспешни опита“;

$W_{20,21} = \neg$ „ $W_{20,22}$ “;

Ядрото, което в позиция влиза L_{18} получава характеристика “Автоматично обработване на транзакциите”.

Ядрото, което влиза в позиция L_{19} получава характеристика “Статус плащането изпратено”.

Ядрото, което влиза в позиция L_{20} получава характеристика “Статус неуспешно броене ≥ 5 ”.

Ядрото, което влиза в позиция L_{21} получава характеристика “Успешна потребителска транзакция”.

Ядрото, което влиза в позиция L_{22} получава характеристика “Статус повторен опит за плащане”.

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

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

където:

$W_{17,23}$ = „Налице е успешно завършила транзакция“;

$W_{17,24}$ = „Транзакцията е завършила, но с грешки“;

$W_{17,25}$ = „Транзакцията е завършила с 0 изтеглени“;

$W_{21,23}$ = „ $W_{17,23}$ “;

$W_{21,24}$ = „ $W_{17,24}$ “;

$W_{21,25}$ = „ $W_{17,25}$ “;

Ядрото, което влиза L_{23} получава характеристика
“Статус завършен”.

Ядрото, което влиза L_{24} получава характеристика
“Статус завършен с грешка”.

Ядрото, което влиза L_{25} получава характеристика
“Статус завършен (0 sum)”.

3.2 ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА СТАНДАРТЕН ИНТЕРНЕТ ПОРТАЛ ЗА ЕЛЕКТРОННО РАЗПЛАЩАНЕ С ПОМОЩТА НА ИНТУИЦИОНИСТКИ РАЗМИТИ ОЦЕНКИ

Представена е теория за интуиционистки размити оценки.

Тук ще използваме Интуиционистките размити множества и в частност Интуиционистките размити оценки. Те са необходими за да ни дадат възможност да преценим вероятни повреди в системата. Оценка се представят по наредени двойки $\langle \mu, \nu \rangle$ на реални числа от множеството $[0,1]$.

S - са всички възможни пакети информация, които се движат в системата.

S_1 - са пакетите с информация, които успешно достигат до местоназначението си.

S_2 - са пакетите с информация, които по неизвестна причина не достигат до местоназначението си.

Степента на несигурност $\pi = 1 - \mu - \nu$ това са всички пакети с информация в платежната система, които преминават успешно и всички възможни неуспешни въвеждания.

В крайна сметка, разплащателните портали [49] улесняват комуникацията между уебсайтовете и физическите магазини, като се използва разплащателният алгоритъм на банката, издава кредитната карта, която е нужна за завършването на покупката.

Първоначално, в обобщената мрежа постъпват следните ядра:

в $L_1 - A$ - ядро с характеристика

“Клиент”;

в $L_2 - B$ - ядро с характеристика

“База данни с информация за кредитни карти”;

в $L_3 - B_1$ - ядро с характеристика

“База данни с потребителски акаунти”;

в $L_4 - B_2$ - ядро с характеристика

“База данни с търговски акаунти”;

- в $L_7 - \zeta$ -ядро с характеристика
“Стоки/услуги”;
- в $L_9 - B_3$ -ядро с характеристика
“Баланс по сметка”;
- в $L_{10} - B_4$ -ядро с характеристика
“Резултат от проверка на търговски акаунт”;
- в $L_{16} - G$ -ядро с характеристика
“Доставка на стока ”;
- в $L_{17} - G_1$ -ядро с характеристика
“Потвърждаване на доставката ”;
- в $L_{18} - \Gamma$ -ядро с характеристика
“Изход”;
- в $L_{19} - A_1$ -ядро с характеристика
“Възможна неуспешна оторизация”;
- в $L_{20} - A_1$ -ядро с характеристика
“Възможно неуспешно плащане”;
- в $L_{21} - A_1$ -ядро с характеристика
“Възможна неуспешна доставка”;

GN модел на стандартен разплащателен портал (Фиг. 3.2) е представен от множеството от преходи:

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

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“.

OM моделът на стандартен разплащателен портал съдържа следните преходи:

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

$R_1 =$	L_2	L_3	L_4	L_5	L_6	L_{19}
L_1	<i>true</i>	<i>false</i>	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>
L_2	<i>true</i>	$W_{2,3}$	<i>false</i>	$W_{2,5}$	$W_{2,6}$	$W_{2,19}$
L_3	<i>false</i>	<i>true</i>	<i>false</i>	$W_{3,5}$	$W_{3,6}$	$W_{3,19}$
L_{11}	<i>false</i>	<i>false</i>	$W_{11,4}$	<i>false</i>	<i>false</i>	<i>false</i>

където:

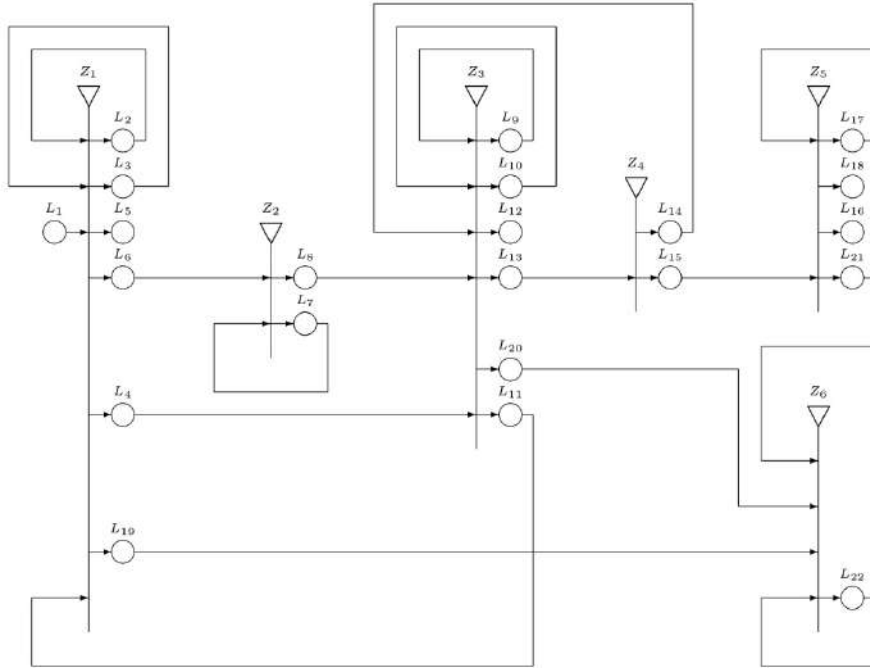
- $W_{2,3} =$ „Наличен е клиентски акаунт“;
 - $W_{2,5} = \neg W_{2,3}$;
 - $W_{2,6} =$ „Позициите L_2, L_3, L_4 не могат за завършват“;
 - $W_{3,5} =$ „Възникнал е проблем с дебитна/кредитна карта”;
 - $W_{3,6} = W_{2,6}$;
 - $W_{11,4} =$ „Потвърден акаунт на търговеца“.
 - $W_{2,19} =$ „Неуспешна оторизация 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. 3.2 OM на интернет портал за електронно разплащане (PGW)

$$Z_2 = \langle \{L_6, L_7\} \{L_7, L_8\}, R_2, \wedge (L_6, L_7) \rangle,$$

$$R_2 = \begin{array}{c|cc} & L_7 & L_8 \\ \hline L_6 & true & false \\ L_7 & true & true \end{array},$$

където:

Ядрото което постъпва в позиция L_6 получава характеристика “Клиент/посетител”.

Ядрото което постъпва в позиция L_7 получава характеристика “Стоки/услуги”.

Ядрото което постъпва в позиция L_8 получава характеристика “Клиент/посетител”.

$$Z_3 = \langle \{L_8, L_9, L_{10}, L_4, L_{14}\} \{L_{12}, L_9, L_{10}, L_{13}, L_{11}, L_{20}\}, R_3, \vee (L_8, L_9, L_{10}, L_4, L_{14}) \rangle,$$

$$R_3 = \begin{array}{c|cccccc} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{20} \\ \hline L_4 & false & true & false & false & false & false \\ L_8 & true & false & false & false & false & false \\ L_9 & true & W_{9,10} & false & W_{9,12} & false & W_{9,20} \\ L_{10} & false & true & true & W_{10,12} & W_{10,13} & false \\ L_{14} & true & false & false & false & false & false \end{array},$$

където:

$W_{9,12} =$ „Установен е недостиг на средства“;

$W_{9,10} = \neg W_{9,12}$;

$W_{9,20} =$ „Възникнала е неидентифицирана грешка с банковата сметка “;

$W_{10,12} =$ „Съществува проблем с акаунта на търговеца“;

$W_{10,13} = \neg W_{10,12}$.

Ядрото което постъпва в позиция L_9 получава характеристика
“Баланс по сметка”.

Ядрото което постъпва в позиция L_{10} получава характеристика
“База данни търговски акаунти ”.

Ядрото което постъпва в позиция L_{11} получава характеристика
“Отговор към L_4 ”.

Ядрото което постъпва в позиция L_{12} получава характеристика
“Грешка Изход”.

Ядрото което постъпва в позиция L_{13} получава характеристика
“Клиент/посетител”.

$$Z_4 = \langle \{L_{13}\} \{L_{14}, L_{15}\}, R_4, \wedge (L_{13}) \rangle,$$

$$R_4 = \begin{array}{c|cc} & L_{14} & L_{15} \\ \hline L_{13} & true & true \end{array}$$

където:

Ядрото което постъпва в позиция L_{14} получава характеристика
“удръжка на средства по Кредитна/Дебитна карта”.

Ядрото което постъпва в позиция L_{15} получава характеристика
“Клиент/посетител”.

$$Z_5 = \langle \{L_{15}, L_{17}\} \{L_{16}, L_{17}, L_{18}, L_{21}\}, R_5, \vee (L_{15}, L_{17}) \rangle,$$

$$R_5 = \begin{array}{c|cccc} & L_{16} & L_{17} & L_{18} & L_{21} \\ \hline L_{15} & false & true & false & false \\ L_{17} & W_{17,16} & false & W_{17,18} & W_{17,21} \end{array}$$

където:

$W_{17,16} =$ „Доставката е успешна“;

$W_{17,18} = \neg W_{17,16}$

$W_{17,21} =$ „Съществува неидентифицирана грешка“;

Ядрото което постъпва в позиция L_{16} получава характеристика
“Доставка на стоки/услуги”.

Ядрото което постъпва в позиция L_{17} получава характеристика
“Потвърждаване на доставката”.

Ядрото което постъпва в L_{18} получава характеристика
“Изход”.

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

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

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 $\langle \mu_k, \nu_k \rangle$ ”.

Първоначално, когато не е получена информация от позиции $L_{19}, L_{20}, L_{21}, L_{22}$, всички оценки приемат първоначални стойности от $\langle 0, 0 \rangle$ а когато $k \geq 0$, текущата $(k + 1)$ -ва оценка е изчислена на базата на предишните оценки според рекурсивната формула:

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

Порталът за електронно разплащане се използва за улесняване на онлайн транзакциите и им позволява да бъдат одобрени. Това е и първото място, където транзакцията постъпва, когато клиент подаде поръчка онлайн. Моделът е представен с обобщена мрежа и показва потоците на транзакциите през портала за електронно разплащане, както и чрез различни проверки, одобрения и възможни откази. Така обобщеномрежовият модел ни помага да погледнем по-нататък в шлюза и да коригираме възможни проблеми, да симулираме други проблеми или просто да го използваме за оптимизиране на поведението на портала за електронно разплащане.

3.3 ОБОБЩЕНОМРЕЖОВ МОДЕЛ ЗА ОЦЕНКА НА РИСКА ОТ КИБЕР-ВМЕШАТЕЛСТВО ВЪРХУ ДРОНОВЕ ЧРЕЗ ИЗПОЛЗВАНЕТО НА ИНТУИЦИОНИСТКИ РАЗМИТИ ОЦЕНКИ

Представена е теория за комуникацията на дроновете.

Възможната комуникационна намеса може да произтича от смущения в комуникацията между RX контролерът и TX приемникът. Моделът OM [9, 40] ще ни помогне лесно и ясно да разберем основните режими на работа от етапите на комуникация на предавателя и приемника на безпилотния хеликоптер както и възможното външно вмешателство, така че да можем да успеем да подобрим сигурността, отстраняване на неизправности в системата както и по-добро анализиране на целия процес.

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 интуиционистки размити множества, за да преценим възможното вмешателство в комуникацията.

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

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

където:

S - Всички възможни опити за TX-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.

Процесът на комуникация между UAV радиопредавателят TX и RX радиоприемникът и обратната комуникация.

Първоначално в обобщената мрежа постъпват следните ядра:

в позиция $L_1 - A$ – постъпва ядро с начална характеристика

“Потребител”;

в позиция $L_2 - \beta$ - постъпва ядро с начална характеристика

“Предавател БД команди;

в позиция $L_8 - \beta''$ - постъпва ядро с начална характеристика

“БД обработка на протоколи”;

в позиция $L_{11} - \beta'''$ - постъпва ядро с начална характеристика

“База данни обработка на канали ”;

в позиция $L_{13} - \chi$ - постъпва ядро с начална характеристика

“Комуникационен канал на дрона / скенер на протоколи ”;

в позиция $L_{14} - \beta''''$ - постъпва ядро с начална характеристика

“БД обработка на приемника ”;

в позиция $L_{19} - \alpha$ - постъпва ядро с начална характеристика

“Процесор дрон ”;

в позиция $L_{23} - \delta$ - постъпва ядро с начална характеристика

“IFE оценки $\langle \mu_k, \nu_k, \pi \rangle$ ”;

OM – модел UAV OM модел на стандартен комуникационен процес между [48, 63, 64, 68, 72, 78, 81, 83, 86, 89] радиопредавател Tx и Rx [60, 74, 82, 91, 102] радиоприемник.

Фигура 3.3 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 предавателя”;

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“.

ОМ модел на стандартен комуникационен процес между UAV радиопредавател.

T_x и R_x [60, 74, 82, 91, 102] радиоприемник и обратна комуникация както и възможно външно вмешателство.

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

	L_2	L_3	L_4	L_5	
$R_1 =$	L_1	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>
	L_2	<i>true</i>	<i>true</i>	$W_{2,4}$	<i>false</i>
	L_7	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>
	L_{10}	<i>true</i>	<i>false</i>	<i>false</i>	<i>false</i>
	L_{18}	<i>false</i>	<i>false</i>	$W_{18,4}$	<i>true</i>

където:

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

$W_{18,4} =$ „Има телеметрична R_x грешка в сигнала“;

Ядрото, което постъпва в позиция L_2 получава характеристика
„БД команди предавател“;

Ядрото, което постъпва в позиция L_3 получава характеристика
„Комуникационна команда изпратена към приемника“;

Ядрото, което постъпва в позиция L_4 получава характеристика
„Изход, грешка“;

Ядрото, което постъпва в позиция L_5 получава характеристика
„Предавател аудио/видео екран“;

$$Z_2 = \langle \{L_8\} \{L_6, L_7, L_8\}, R_2, \wedge (L_8) \rangle,$$

	L_6	L_7	L_8	
$R_2 =$	L_8	<i>true</i>	<i>true</i>	<i>true</i>

където:

Ядрото, което постъпва в позиция L_6 получава характеристика
„Протоколна команда изпратена до предавателя“;

Ядрото, което постъпва в позиция L_6 получава характеристика
„Протоколна команда изпратена до предавателя“;

Ядрото, което постъпва в позиция L_7 получава характеристика
„Протоколна команда изпратена до приемника“;

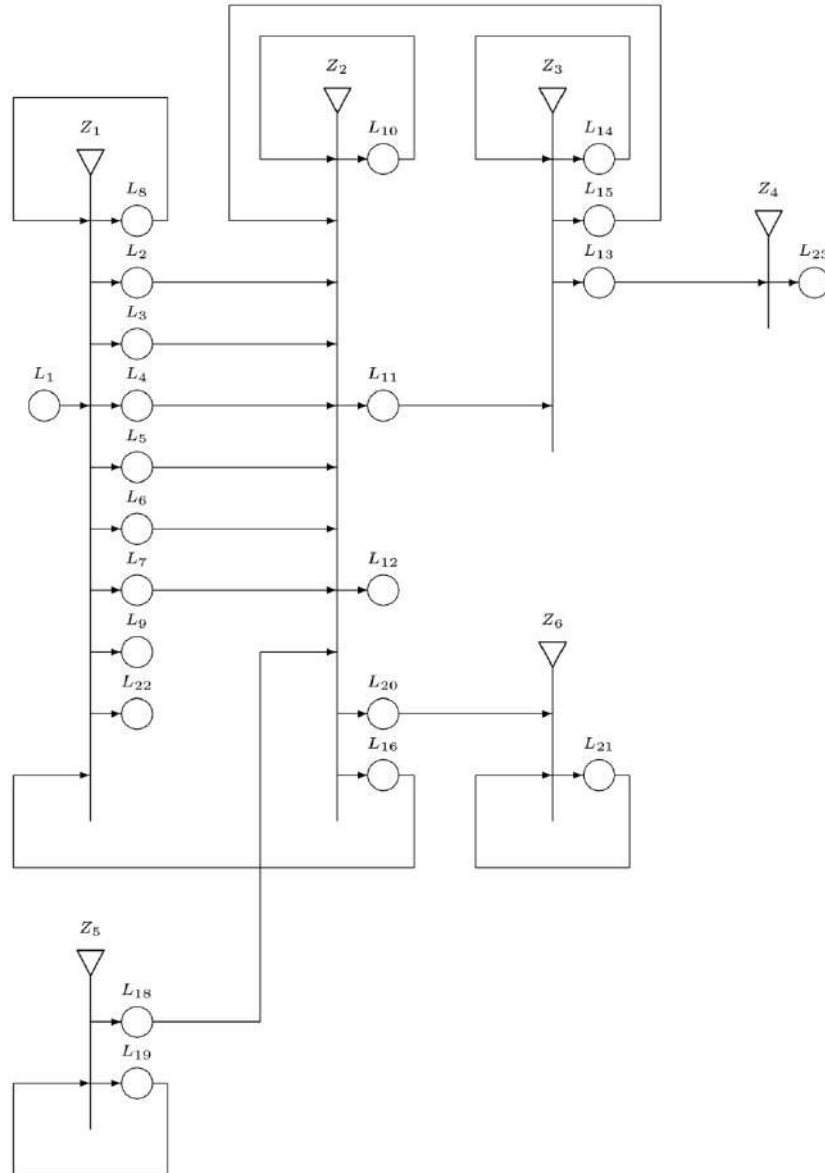
Ядрото, което постъпва в позиция L_6 получава характеристика
„Протоколна команда изпратена до предавателя“.

Ядрото, което постъпва в позиция L_7 получава характеристика
„Протоколна команда изпратена до приемникът“.

Ядрото, което постъпва в позиция L_8 получава характеристика
„База данни за обработка на протоколи“.

Ядрото, което постъпва в позиция L_6 получава характеристика
„Протоколна команда изпратена до предавателя“.

Ядрото, което постъпва в позиция L_7 получава характеристика
„Протоколна команда изпратена до приемника“.



Фигура 3.3 Обобщеномрежови модел за оценка на риска от кибер-вмешателство върху дронове

$$Z_3 = \langle \{L_{11}\} \{L_9, L_{10}, L_{11}\}, R_3, \wedge (L_{11}) \rangle,$$

$$R_3 = \frac{}{L_{11}} \left| \begin{array}{ccc} L_9 & L_{10} & L_{11} \\ \hline true & true & true \end{array} \right.,$$

където:

Ядрото, което постъпва в позиция L_8 получава характеристика “База данни за обработка на протоколи”.

Ядрото, което постъпва в позиция L_9 получава характеристика “Команда за избор на канал е изпратена до приемникът”.

Ядрото, което постъпва в позиция L_{10} получава характеристика “Команда за избор на канал е изпратена до предавателя”.

Ядрото, което постъпва в позиция L_{11} получава характеристика “База данни за обработка на канали”.

$$Z_4 = \langle \{L_{13}\} \{L_{12}, L_{13}\}, R_4, \vee (L_{13}) \rangle,$$

$$R_4 = \frac{L_{12} \quad L_{13}}{L_{13} \quad \left| \begin{array}{cc} & \\ true & true \end{array} \right.},$$

където:

Ядрото, което постъпва в позиция L_{12} получава характеристика
“Нарушител на външната комуникация”;

Ядрото, което постъпва в позиция L_{13} получава характеристика
“Комуникация дрон сканиране на канали/протоколи”;

$$Z_5 = \langle \{L_3, L_6, L_9, L_{12}, L_{14}, L_{20}\} \{L_{14}, L_{15}, L_{16}, L_{17}, L_{18}\}, R_5, \wedge (L_3, L_6, L_9, L_{12}, L_{14}, L_{20},) \rangle,$$

R_5	L_{14}	L_{15}	L_{16}	L_{17}	L_{18}
L_3	true	false	false	false	false
L_6	true	false	false	false	false
L_9	true	false	false	false	false
L_{12}	true	false	$W_{12,16}$	true	false
L_{14}	true	$W_{14,15}$	$W_{14,16}$	true	false
L_{20}	false	false	$W_{20,16}$	false	true

където:

$W_{14,15}$ = „Има успешно изпратена TX команда“;

$W_{12,16}$ = „Атаката на нарушителят е неуспешна“;

$W_{14,16}$ = „ $W_{14,15}$ “;

$W_{20,16}$ = „Има грешка в RX телеметричния сигнал“;

Ядрото, което постъпва в позиция L_{14} получава характеристика
“База данни за обработка на приемника”;

Ядрото, което постъпва в позиция L_{15} получава характеристика
“Успешно предаден сигнал към процесора”

Ядрото, което постъпва в позиция L_{16} получава характеристика
“Грешка/изход”;

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

Ядрото, което постъпва в позиция L_{18} получава характеристика
“Rx - обратен комуникационен телеметричен монитор”.

$$Z_6 = \langle \{L_{15}, L_{19}\} \{L_{19}, L_{20}, L_{21}\}, R_6, \wedge (L_{15}, L_{19}) \rangle,$$

R_6	L_{19}	L_{20}	L_{21}
L_{15}	true	false	false
L_{19}	true	$W_{19,20}$	$W_{19,21}$

където:

$W_{19,20}$ = „Налице е успешен телеметричен RX обратен комуникационен сигнал, изпратен към предавателя“;

$W_{19,21}$ = „Налице е успешно предадена команда към дрона“;

Ядрото, което постъпва в позиция L_{19} получава характеристика
“Процесор - дрон”.

Ядрото, което постъпва в позиция L_{20} получава характеристика
“Телеметрия на приемника”.

Ядрото, което постъпва в позиция L_{21} получава характеристика “Предадена команда на дронът която е реализирана в маневра ”.

$$Z_7 = \langle \{L_{21}\} \{L_{22}\}, R_4, \vee (L_{21}) \rangle,$$

$$R_7 = \frac{L_{22}}{L_{21} \mid true},$$

където:

Ядрото, което постъпва в позиция L_{22} получава характеристика “Дрона е в работен режим”.

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

$$R_8 = \frac{L_{23}}{L_{17} \mid true},$$

$$L_{23} \mid true$$

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 $\langle \mu_k, \nu_k \rangle$ ”.

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

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

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

където $\langle \mu_k, \nu_k \rangle$ е предишната оценка, и $\langle \mu, \nu \rangle$ е последната оценка на възможната външна намеса в комуникацията, 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 МОДЕЛИРАНЕ НА ЗАХРАНВАЩАТА И ОХРАНИТЕЛНА СИСТЕМА НА SMART HOUSE

Представена е теория за Smart house.

В този раздел е описан Обобщеномрежовият модел на електрическата инсталация и охранителната система на Smart house и е представено функционирането им. Обобщеномрежовият модел е редуциран (виж [3, 24]). Той съдържа $n + 6$ прехода, $3n + L_7$ места, където n е броят на електрическите уреди, а $L_4 + n$ типа ядра (виж Фиг. 1). Значението на тези ядра е обяснено по-долу. Ядрото ρ представлява регулатора, остава постоянно на позиция L_6 и приема характеристика “интелигентна система (параметри)”.

Ядрото β представлява батерията, остава постоянно на позиция L_{12} и приема характеристика “батерия (параметри), първоначален капацитет на батерията”.

Ядрото π представлява системата за сигурност, остава постоянно на

позиция L_{15} с начална характеристика “система за сигурност (параметри), първоначално състояние”. Ядра $\alpha_1, \dots, \alpha_n$ представляват различните уреди (напр. печка, бойлер, климатик и др.), остават постоянно на позиции L_{18}, \dots, L_{3n+15} . i -тата лексема има характеристика „ i -ти електрически уред (параметри, напр. консумация на енергия)“ на място L_{3i+15} за $i = 1, \dots, n$.

Ядрата к постъпват на позиция L_1 с начална характеристика „осигурена електрическа мощност (ват (W))“. Във всеки един момент от време, ако има електричество в Smart house, постъпва ядро ϵ място L_7 с начална характеристика „Smart house има електричество“. Формалното описание на преходите на мрежата е дадено по-долу.

$$Z_1 = \langle \{L_1, L_6, L_{11}, L_{14}, L_{19}, \dots, L_{3n+16}\}, \{L_2, L_3, L_4, L_5, L_6\} \rangle,$$

$R_1 =$	L_2	L_3	L_4	L_5	L_6
L_1	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
L_6	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
L_{11}	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
L_{14}	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
L_{19}	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
L_{3n+16}	<i>false</i>	<i>false</i>	<i>false</i>	<i>false</i>	<i>true</i>
L_6	$W_{6,2}$	$W_{6,3}$	$W_{6,3}$	$W_{6,4}$	<i>true</i>

където:

$W_{6,2}$ = “Има сигнал за включване/изключване на електрически уред”,

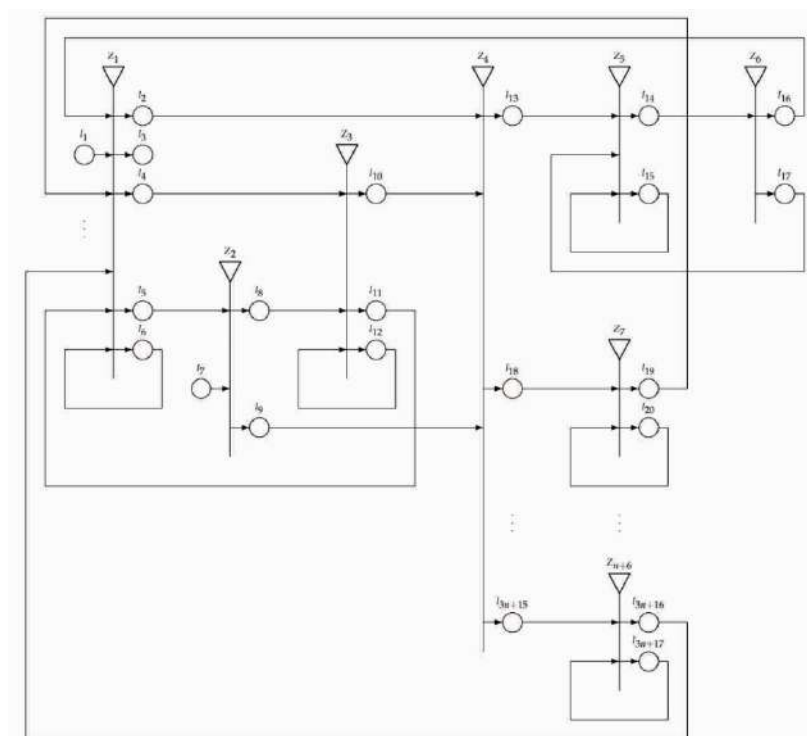
$W_{6,3}$ = “Има сигнал от СОР ”,

$W_{6,4}$ = “Има сигнал за захранване на системата”,

$W_{6,5}$ = “Има сигнал за управление на батерията”

Ядрото к постъпва на позиция L_6 и се обединява с ядрото p , която получава характеристиката

„общо текущо състояние на системата, включително интелигентната система за сигурност ”.



Фиг. 3.4 GN модел на функциониране на електрозахранването и сигурността на интелигентната къща

В следващият момент (според началната характеристика на ρ или текущото състояние на системата), ядрото ρ се разделя на две ядра - същото ядро ρ , което продължава до остава на позиция L_6 и ядрото σ_j за $j = 1, 2, 3, 4$.

Ядрото ρ получава характеристиката

„времеви момент; текущата команда, която е характеристиката на токена σ_j ”.

Когато моментът за включване/изключване на COT или i -тия апарат е достигнат, ядрото σ_1 постъпва на позиция L_2 и получава характеристиката

„времеви момент; съответният апарат трябва да бъде включен/изключен”.

В първия тип извънредни случаи, когато няма текущо ϵ -ядро и ниво на електричество от текущата β -характеристика е ниско, сигналът към всички уреди с изключение на системата за сигурност е „изключване“. Във втория вид извънредни случаи, когато има сигнал (γ_i), че има инцидент с i -тия апарат, ядрото σ_1 постъпва на позиция L_2 и получава характеристиката

„времеви момент; i -тия апарат трябва да бъде изключен”.

Ако има информация от системата за сигурност, че е задействана, ядрото σ_2 постъпва на място L_3 и получава характеристиката

„сигнал до екипа за обслужване на системата за сигурност за събитие“.

Ако ядрото ϵ в този момент получи характеристиката

„няма текущ токен ϵ , т.е. електричеството спира“.

Ядрото σ_3 постъпва на позиция L_4 с характеристиката

„сигнал към батерията за започване на подаване на електричество“.

Ако има информация от батерията (сигнал σ_5), че нивото на електрическата енергия в батерията е ниска/висока, ядрото σ_4 постъпва на позиция L_5 и получава характеристиката

„сигнал за зареждане/незареждане на батерията“.

$$Z_2 = \langle \{L_5, L_7\}, \{L_8, L_9\}, L_5 \mid \begin{array}{cc} L_8 & L_9 \\ \hline true & false \\ L_7 & W_{7,8} \quad true \end{array} \rangle,$$

Където:

$W_{7,8}$ = „Има ядро на позиция L_5 “.

Във всеки един момент от време, ако има текущо ядро ε на позиция L_7 , то постъпва на позиция L_9 , но когато ядрото σ_4 постъпва на позиция L_5 с характеристика

„сигнал, че електричеството трябва да бъде насочено към батерията“,

ядрото ε се разделя на две ядра - същото ядро ε , което постъпва на позиция L_9 без нова характеристика, и ядро ε_1 , което постъпва на позиция L_8 и се обединява с ядрото σ_4 с характеристика

„електричество за батерията“.

$$Z_3 = \langle \{L_4, L_8, L_{12}\}, \{L_{10}, L_{11}, L_{12}\}, \begin{array}{ccc} & L_{10} & L_{11} & L_{12} \\ \hline L_2 & false & false & true \\ L_8 & false & false & true \\ L_{12} & W_{10,12} & W_{12,11} & true \end{array} \rangle,$$

Където:

$W_{12,10}$ = „Ако има сигнал от интелигентната система на Smart house за електричество от батерия“,

$W_{12,11}$ = „Ако нивото на заряда в батерията е ниско“.

Ядрото ε_1 постъпва на позиция L_{12} и се обединява с ядрото β , като то получава характеристика

„текущо ниво на заряд в батерията“.

В следващият момент след постъпването на ядрото σ_3 , ако нивото на батерията не е ниско, ядрото β се разделя на две ядра - същото ядро β , което продължава да стои на позицията си L_{12} и ядрото ε_2 , което постъпва на място L_{10} без характеристика.

Ако нивото на заряд в батерията е ниско, ядрото β се разделя на две ядра - същото ядро β , което продължава да остава на позиция L_{12} , и ядрото σ_5 , което постъпва на позиция L_{11} с характеристика

„ниско ниво на батерията“.

$$Z_4 = \langle \{L_2, L_9, L_{10}\}, \{L_{13}, L_{16}, \dots, L_{3n+13}\} \rangle,$$

$$R_4 = \begin{array}{c|cccc} & L_{13} & L_{16} & \dots & L_{3n+13} \\ \hline L_2 & W_{2,13} & W_{2,16} & \dots & W_{2,3n+13} \\ L_9 & W_{9,13} & W_{9,16} & \dots & W_{9,3n+13} \\ L_{10} & W_{10,13} & W_{10,16} & \dots & W_{10,3n+13} \end{array},$$

Където:

$W_{2,13}$ = „Има сигнал от системата на Smart house за включване/изключване на система за сигурност“,

$W_{2,3i+13}$ = „Има сигнал от системата на Smart house за включване/изключване на i -

ти апарат” ($i = 1, \dots, n$),

$W_{9,13}$ = „Последният сигнал от системата за интелигентен дом е за включване на охранителната система”,

$W_{9,3i+13}$ = „Последният сигнал от системата за интелигентен дом е за включване на i -тия апарат” ($i = 1, \dots, n$),

$W_{10,13}$ = „Няма ε -ядро и последният сигнал от интелигентната система на Smart house е за включване на системата за сигурност”,

$W_{10,3i+13}$ = „Няма ε -ядро и последният сигнал от системата на Smart house е за включване на i -тия апарат” ($i = 1, \dots, n$).

Ядрото σ_1 постъпва на съответната позиция, за което предикатът е верен, заедно със съответното ε -ядро (ε или ε_2) и двете ядра се обединяват без нова характеристика.

$$Z_5 = \langle \{L_{13}, L_{15}, L_{17}\}, \{L_{14}, L_{15}\}, \begin{array}{c|cc} & L_{14} & L_{15} \\ \hline L_{13} & false & true \\ L_{15} & W_{15,14} & true \\ L_{17} & false & true \end{array} \rangle,$$

Където:

$W_{15,14}$ = „Има авария/техническа повреда на системата за сигурност”.

$W_{15,14}$ = „Ако е true, ядрото π се разделя на две ядра — същото ядро π , което продължава да остава на позиция L_{15} с характеристика

„текущо състояние на системата за сигурност“

и ядрото γ , което постъпва на позиция L_{14} с характеристика

„има инцидент, регистриран от системата за сигурност“.

$$Z_6 = \langle \{L_{14}\}, \{L_{16}, L_{17}\}, \begin{array}{c|cc} & L_{16} & L_{17} \\ \hline L_{14} & W_{14,16} & W_{14,17} \end{array} \rangle,$$

Където:

$W_{14,16} = \neg W_{14,17}$,

$W_{14,17}$ = „Регистрираният от системата за сигурност инцидент е преминал през повторна проверка”,

Където $\neg P$ е отрицанието на предиката P .

$W_{14,16} = true$, ядрото π постъпва на позиция L_{16} с характеристика

„има инцидент, регистриран от системата за сигурност“, докато на позиция L_{17} не се получава нова характеристика.

Важно е да се отбележи, че процесът на проверката на инцидента, регистриран от системата за сигурност може да бъде описана подробно от обобщенорежови модел, подобно на модела, описан в [42].

За всяко $i = 1, \dots, n$:

$$Z_{i+6} = \langle \{L_{3i+15}, L_{3i+17}\}, \{L_{3i+16}, L_{3i+17}\}, \begin{array}{c|cc} & L_{3i+16} & L_{3i+17} \\ \hline L_{3i+15} & false & true \\ L_{3i+17} & W_{3i+17,3i+16} & true \end{array} \rangle,$$

където:

$W_{3i+17,3i+16}$ = „Има авария/техническа повреда на системата за сигурност”.

Когато $W_{3i+17,3i+16} = true$, ядрото α_i се разделя на две ядра - същото ядро α_i , което

продължава да стои на позиция L_{3i+17} с характеристика „текущо състояние на i -тия апарат“ и ядрото γ_i , което постъпва на позиция L_{3i+16} с характеристика „има инцидент с i -тия апарат“.

Тук за първи път чрез обобщеномрежов модел е описано функционирането на електрическата система и системата за сигурност на Smart house. Разгледани са възможностите за дистанционно управление на определени уреди и системите в Smart house. В обобщеномрежовият модел също е взети предвид необходимостта от интелигентен контрол над Smart house, включително захранването на отделните електрически уреди. Фокусът е върху системата за сигурност и интелигентната система, която управлява целия процес. За тази цел се използват обобщени мрежи като инструмент за моделиране на процеси, протичащи паралелно във времето. В модела е разгледано и допълнителна идентификация в разпознаването на събития. При засичане например на движение, е необходима допълнителна идентификация на засеченото лице, пръстов отпечатък, идентификация чрез ретина на окото и други.

Предложеният обобщеномрежови модел може да бъде включен в по-сложен обобщеномрежови модел на смарт квартал и интелигентен град (виж [41]). Може лесно да се адаптира за оценка на икономически показатели като разходите за живот или за оценка на QoS следвайки подхода от [6].

3.5 ИЗВОДИ

В глава трета разгледахме някои системи, свързани със сигурността на интелигентния дом, както и процесите на Data Mining, протичащи в тях. Видяхме, че възможността за дистанционно контролиране и управление на процеси по контрол на достъп и охрана от дистанция са както голямо предимство, така и слабо място във всеки ИД ако не се обърне внимание и не се повиши в значителна степен нивото на сигурност. Посредством интуиционистка размита оценка изследвахме възможностите за проникване в комуникацията и съответно на намеса в управлението, а чрез процесите на Data Mining получихме информация за възможностите и начините за проникване. Друго казано софтуерите, които ще осигуряват достъп, охраняват или извършват разплащания, както и ще управляват интелигентния дом трябва да бъдат съобразени със съвременните изисквания и стандарти за сигурност. Демонстрирахме, че най-важното при тези системи е необходимостта от изключително прецизна защита на комуникацията както със самата система, така и с отделните модули за да не се допусне намесата на недоброжелател, който може да им навреди.

ЗАКЛЮЧЕНИЕ

Напредналите технологии и високото технологично развитие през последните десетилетия неминуемо поставиха темата за „интернет на нещата“ на дневен ред. Силното развитие в тази посока, високата индустриализация на обществото, както и внедряването на най-различни технологии и техники във всяка област на нашия живот, неминуемо поставиха темата за развитието на интелигентните решения в нашето ежедневие. В стремежа си да постигнем максимален комфорт или максимално прецизна система все повече се акцентира на технологиите, естествено придружени и с модерни софтуери. Така се наложиха всички нови технологии в живота и ежедневието ни. Но разбира се те са несъвършени и естественият стремеж на човека към съвършенство ни кара да работим все повече в посока на усъвършенстване и модернизирани на съществуващите системи. И както видяхме в разработката във втора и трета глава, една от посоките на развитие е самоанализът и самообучението на системите, не без помощта на потребителя с неговите корекции и навици. Посока, в която е необходимо да се вложат изключително много усилия, не само в автоматизацията и механизацията, не само в комуникациите между основните системи, но и в сигурността и защитата им.

През последните две десетилетия комуникационните мрежи навлязоха в ежедневието на човечеството. Ежедневно се извършват банкови и финансови операции, покупки посредством интернет, контролират се умните устройства по домовете, както и много други отдалечени действия. По този начин се създадоха предпоставки за всякакви кибер-престъпления, чрез неототоризиран достъп до системите за електронни разплащания и управлението на Smart House, управлението на UAVs и др. Поради тази причина темата за защита от външни посегателства, преки или косвени върху нашият живот е изключително актуална.

В трета глава видяхме как чрез използването на Data mining техники може да се увеличи сигурността и спокойствието, както и да се осигури защитата от неототоризиран достъп до по-горе споменатите системи. Изследванията, които направихме в областта на компютърните и комуникационните мрежи, реализирани с ОМ чрез Data mining техники показаха изключително добри резултати, а също така доказаха, че са надеждно средство, което може да бъде използвано с цел анализ и извличане на данни. По този начин ще минимизираме значително възможностите за проникване в различните системи на интелигентния дом.

С оглед споменатото по-горе в този дисертационен труд е направен кратък обзор на някои резултати в 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 разгледано какво представлява самият процес, както и стандартни техники които се използват и по-конкретно са разгледани стандартните техники за извличането на информация чрез DM.

Направихме програмна симулация на ОМ на реалните процеси, протичащи в автоматизираната осветителна система в ИД чрез софтуера GN IDE. Чрез помощта на този софтуер проведохме симулация на обобщеномрежеви модел и показваме реалните стъпки на всички ядра, тяхното

преминаване през преходите, характеристиките им, както и предикатите, които се случват по време на паралелният процес в самата система. Направихме оценка на риска от кибератака над управлението на SMART HOUSE чрез използването на интуиционистка размита оценка (IFE), като добавихме и 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-вмешателства.

Приноси към дисертационния труд

Основните приноси в този дисертационен труд са с научен, научно-приложен и приложен характер. Те са сведени до създаването и анализирането на обобщеномрежови модели.

Приноси с *научен* характер:

- Разработване на алтернативен метод за автоматизирана настройка и самообучение на осветителната система в "Smart House".
- Разработване на алтернативен метод за оценка на риска от кибер-атаки върху управлението на "Smart House" с помощта на интуционистки размити оценки.
- Разработване и реализация на нов подход за оценка на риска от кибер-вмешателство върху управлението и комуникацията на дроневи чрез използването на интуционистки размити оценки.

Приноси с *научен-приложен* характер:

- Разработване на обобщеномрежов модел на автоматизирана осветителна система в помещение.
- Разработване на обобщеномрежов модел на стандартен интернет портал за електронно разплащане с помощта на интуционистки размити оценки.
- Разработване на обобщеномрежов модел на протичането на реалният разплащателен процес в PGW.
- Разработка на обобщеномрежов 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" разгледахме демонстративната симулация, направена за да покаже действието на автоматизираната система за осветление, като са моделирани вероятности на база корекции върху данните на потребителя. Проследихме процесите от идентификацията на потребителя до включване или изключване на осветлението, като минахме през различните настройки и корекции. Софтуерът GN IDE е разработен специално за нуждите на симулацията на обобщеномрежовите модели, с цел ясна представа, наблюдение и анализ на процесите, които протичат през мрежата. В точка 2.1.2.2 на Глава 2 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 обобщеномрежовият модел.

Насоки за бъдещи изследвания

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

Използване на IFE оценки както и ОМ модели на системата за верификация на „Smart House“ за бъдещо и евентуално предотвратяване на действия на недоброжелатели.

Разработване на облачна структура за управлението на “Smart House“ чрез изграждане ОМ, както и IFE оценки за приоритетно използване на различните уреди в една такава система при наличието на повече от един потребител.

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

Разработване на ОМ оценка на основните фактори при безпилотните летателни устройства БЛУ (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 атмосферните условия преди излитането на БЛУ (Дрон) с цел предотвратяването на грешки при управлението му, както и евентуалната му забрана за излитане с цел ограничаване на възможните грешки и проблеми, които могат да възникнат при неподходящи метеорологични условия.

Нуждата от създаването на ОМ за оценка на риска от кибер-вмешателство в облачната структура на „Smart House“, както и в системата му за интернет разплащания.

Публикации по дисертационния труд

- 1*. 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.
- 2*. 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.
- 3*. 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.
- 4*. 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.
- 5*. 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.
- 6*. Videv T., Hristov G., Bozveliev B. AUTHOR FULL NAMES: Videv, Tihomir; Hristov, Georgi; Bozveliev, Boris. Generalized Net Model of the Network for Automatic Turning and Setting the Lighting in the Room (2020), art. no. 9199847, pp. 526 - 528
- 7*. Videv, Tihomir; Sotirov, Sotir; Bozveliev, Boris. Generalized Net Model of the Network for Automatic Turning and Setting the Lighting in the Room with Intuitionistic Fuzzy Estimations (2020), 862, pp. 83 – 90
- 8*. Tihomir Videv, Sotir Sotirov, Krassimir Atanassov, Velin Andonov. A generalized net model of the electrical power and security functioning of a smart house, Twenty First International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets, Warsaw, Poland, October 20, 2023