Българско списание за
Инженерно Проектиране

брой №43, януари 2021г.

ЦЕЛ И ОБХВАТ

„Българско списание за инженерно проектиране" е периодично научно списание с широк научен и научно-приложен профил. Целта му е да предостави академичен форум за обмен на идеи между учените, изследователите, инженерите, потребителите и производителите, работещи в областта на машиностроенето, транспорта, логистиката, енергетиката, технологиите, съвременното компютърно проектиране, а също така и в областта на различни интердисциплинарни научни и научно-приложни проблеми. Издателите приветстват научни публикации с високо качество и значими научни, научно-приложни и творчески приноси.

РЕДАКЦИОННА КОЛЕГИЯ

Председател
Б. Григоров, ТУ-София, България

М.Т.Георгиев	ТУ-София, България	**К.Деметрашвили**	ТУ, Тбилиси, Грузия
Г.Дюкенджиев	ТУ-София, България	**С.Симеонов**	ТУ, Бърно, Чехия
М.Денчев	ТУ-София, България	**В.Николич**	Университет в Ниш, Сърбия
И.Малаков	ТУ-София, България	**А.Янакиев**	Notingham Trent University, UK
П.П.Петров	ТУ-София, България	**Н.Чернев**	University of Auvergne, France
В.Панов	ТУ-София, България	**B.Lepadatescu**	Transilvania University of Brashov, Romania
М.З.Георгиев	ТУ-София, България	**N.Zrnic**	University of Belgrad, Serbia
Н.Л.Николов	ТУ-София, България	**M.Jovanovic**	University of Nish, Serbia
М.Георгиев	МГТУ Станкин, Москва, Россия	**D.Michalopoulos**	University of Patras, Greece
В.Христов	ТУ-София, България	**N.Kubota**	Tokyo Metropolitan University, Japan
Ch.Apostolopoulos	University of Patras, Greece	**С.Емельянов**	Юго-Западный гос. университет, Курск, Россия
Л.Червяков	Юго-Западный гос. университет, Курск, Россия	**В.Спасов**	ВТУ „Т.Каблешков", София, България
О.Лисовиченко	Национален технически университет, Украйна	**В.Кирилович**	Государственный университет "Житомирская политехника", Украина

Редактор
Р.Митрев, ТУ-София, България

Издател: Машиностроителен факултет, Технически университет-София. ISSN 1313-7530; **Адрес на редакцията:** София, бул.Климент Охридски №8, Технически Университет-София, бл.4, Машиностроителен факултет; **Електронна версия:** bjed.tu-sofia.bg.
Списанието се индексира в Index Copernicus: www.indexcopernicus.com
Всички статии в списанието се рецензират от членове на редакционната колегия и външни специалисти.

Bulgarian journal for
Engineering Design

issue №43, January 2021

AIM AND SCOPE

Bulgarian Journal for Engineering Design is a periodical scientific issue covering wide scientific and application areas of engineering activities. The aim of the journal is to provide an academic forum for exchange of ideas and information between scientists, engineers, manufacturers and customers working in the spheres of mechanical engineering, transport, logistics, power engineering, modern computer – aided design and technology and solving different interdisciplinary scientific and applied problems. The editors welcome articles of substantial quality bearing significant contribution to the engineering knowledge.

EDITORIAL BOARD

Chairman
B.Grigorov, TU-Sofia, Bulgaria

M.T.Georgiev	TU-Sofia, Bulgaria	**K.Demetrashvili**	TU, Tbilisi, Georgia
G.Diukendzhiev	TU-Sofia, Bulgaria	**S.Simeonov**	TU, Brno, Czech Republic
M.Denchev	TU-Sofia, Bulgaria	**V.Nikolich**	Nish university, Serbia
I.Malakov	TU-Sofia, Bulgaria	**A.Ianakiev**	Notingham Trent University, UK
P.P.Petrov	TU-Sofia, Bulgaria	**N.Chernev**	University of Auvergne, France
V.Panov	TU-Sofia, Bulgaria	**B.Lepadatescu**	Transilvania University of Brashov, Romania
M.Z.Georgiev	TU-Sofia, Bulgaria	**N.Zrnic**	University of Belgrad, Serbia
N.L.Nikolov	TU-Sofia, Bulgaria	**M.Jovanovic**	University of Nish, Serbia
M.Georgiev	MGTU Stankin, Moscow, Russia	**D.Michalopoulos**	University of Patras, Greece
V.Hristov	TU-Sofia, Bulgaria	**N.Kubota**	Tokyo Metropolitan University, Japan
Ch. Apostolopoulos	University of Patras, Greece	**S.Emelianov**	South West State University, Kursk, Russia
L.Cherviakov	South West State University, Kursk, Russia	**V.Spassov**	VTU „T.Kableshkov“, Sofia, Bulgaria
O.Lisovychenko	National technical university, Ukraine	**V.Kirilovich**	Zhytomyr Polytechnic State University, Ukraine

Editor
R.Mitrev, TU-Sofia, Bulgaria

Publisher: Mechanical Engineering Faculty, Technical University-Sofia. ISSN 1313-7530; **Publisher Address:** Bulgaria, Sofia, Kliment Ohridski blvd. №8, Technical University-Sofia, Mechanical engineering faculty; **Electronic version:** bjed.tu-sofia.bg.
The journal is indexed in Index Copernicus: www.indexcopernicus.com
All papers are reviewed by the members of Editorial Board and by external specialists.

Българско списание за инженерно проектиране, брой 43, януари 2021г.
Bulgarian Journal for Engineering Design, issue 43, January 2021

Съдържание:

ИНТЕЛИГЕНТНА СИСТЕМА ЗА ДЕТЕКТИРАНЕ НА КОМПРОМЕТИРАНИ IOT УСТРОЙСТВА В РЕЗУЛТАТ НА КИБЕРАТАКА

Александър ХРИСТОВ
катедра „ИТИ", ТУ- София, България
e-mail: ahristov@tu-sofia.bg

Резюме: Целта на настоящата статия е да се предложи система за детектиране на компрометирани IoT устройства в резултат на кибератака. Предложената интелигентна система използва Wavelet трансформации и филтър на Haar. Системният монитор записва синхронно във времето индекси за натоварването на процесор, памет и мрежов порт). Записват се синхронно във времето индексите на нормално работещи IoT устройства и тези индексите на компрометирани устройства при някои конкретни широкоизвестни кибератаки в интернет на нещата. След което, използвайки така получените индекси се уточняват параметрите на системата, така че да се разграничават (филтрират) двете състояния на IoT устройствата- нормално работещи или компрометирани.

Ключови думи: Информационна сигурност, Системи с изкуствен интелект, Интернет на нещата, Wavelet, IoT устройства

1. ВЪВЕДЕНИЕ

Днес информационните и комуникационни технологии се превръщат в основа на всички дейности в икономиката, администрацията, обществото и личния живот. Дигиталните инфраструктури [1] се превръщат от поддържаща среда в основен и критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на развитието на конкурентна и иновативна икономика, прозрачно управление и на модерно демократично гражданско общество.

Непрекъснато нараства интересът към Интернет на нещата (IoT), към Индустриалния интернет на нещата (IIoT) и в частност информационната сигурност [2] на IoT устройства.

Извършеният литературен обзор показа, че в световен мащаб проблемът за информационната сигурност на IoT устройствата е все още слабо разработен [2, 3, 4 и цитираната там литература] и липсват достъпни системи за детектиране на компрометирани IoT устройства в резултат на кибератака, поради което се счита, че получените резултати ще бъдат с национално и международно значение, имайки предвид Националната стратегия за научни изследвания и обществените предизвикателства, определени в нея, както и институционалните и европейски приоритети.

В [4] е предложен един конкретен подход за идентифициране на компрометирани устройства в резултат на кибератака, който се базира на мониторинг на използването на процесорните ядра, паметта и мрежовия комуникационен интерфейс за определяне състоянието (компрометирано/некомпрометирано) на IoT устройствата. Решаващото правило (функция, разделяща пространството на две непресичащи се множества) на алгоритъма намира съответствието на състоянието от постъпващите времеви редове от стойности. Особеност на подхода е предобработката, т.е. използвайки обучаващи извадки от времевите редове от стойности (използването на процесор, памет и мрежов интерфейс) се определят три клъстерни области и центъра на всеки от трите клъстера. Първият клъстер съответства на некомпрометирано състояние, а вторият и третият съответстват на състояния след SQL Injection, като се реализира филтрация по предварително зададено поле на таблицата, или се реализира добавяне на данни към таблица след преобразуването им. Предимство на горния подход е, че се разграничават тези две конкретни състояния, а недостатък, че не може да идентифицира всевъзможните други компрометирани състояния на IoT устройството.

Целта на настоящата работа е на базата на анализ на методите и средствата на системите за информационна сигурност чрез инструменти с

научно – приложен характер да се разработи модел за идентифициране на компрометирани устройства в резултат на кибератака в IoT.

2. МЕТОД ЗА ИДЕНТИФИЦИРАНЕ НА КОМПРОМЕТИРАНИ СЪСТОЯНИЯ

По- долу се предлага универсален метод за идентифициране на различни компрометирани състояния. Методът използва коефициенти, получени от Wavelet трансформация за процентното натоварване на паметта на IoT устройството.

Wavelet трансформацията [5] е трансформация, която осигурява едновременно представяне на сигнала във времева и честотна област. Тя предава сигнал във времевата област през високочестотен и нискочестотен филтри, като филтрира съответно ниската и високата честота на сигнала. Процедурата се повтаря, докато част от сигнала, съответстващ на дадена честота, се премахва от сигнала. Процедурата се нарича разлагане. Разлагането се повтаря до предварително зададено ниво на декомпозиция. След това се образува множество от сигнали, които всъщност представят оригиналния сигнал.

За натоварването на паметта на IoT устройството, следва да се използва Wavelet дискретното преобразуване. Haar трансформацията [5] разлага дискретния сигнал на два подсигнала. Единият подсигнал е текущата средна стойност или тенденция T; другият подсигнал е текущата разлика или флуктуация d.

Енергията на тенденцията на подсигнала T се счита за по-голямата част от енергията на преобразувания сигнал [5]. Следователно, може да се пресметне енергията, отчитайки само коефициентите на тенденцията на първото ниво на разлагането:

$$E_T = \sum_{j=1}^{n} T_j^2 \qquad (1)$$

Алгоритъм

Методът за идентифициране на различни компрометирани състояния на IoT устройствата използва като мярка енергията [5] чрез Wavelet трансформацията върху натоварването на паметта на IoT устройството. Методът за тестване се състои от две фази. В първата фаза (Първоначална фаза), Wavelet енергийната стойност на некомпрометираното IoT устройство се измерва и запаметява. Във втората фаза (Тестова фаза), Wavelet енергията на тестваното IoT устройство се измерва и сравнява със съответната стойност получена през първата фаза. Идентифицирането на различни компрометирани състояния ще бъде успешна, когато Wavelet енергията превишава дадени граници на толеранс. Тези граници са въведени, за да се вземат под внимание вариациите на натоварването на паметта на IoT устройството при различни компрометирани състояния и неточностите от измерването (системния монитор).

Опционално, накрая може итеративно да се обновяват дефинициите на Wavelet енергията за некомпрометирано IoT устройство и границите на толеранс за откриване на компрометираните състояния. Дадено е множество от n на брой некомпрометирани състояния на IoT устройството, множеството $E_{T,i}$ е енергийната стойност за натоварването на паметта на IoT устройството при различни некомпрометирани състояния, $E_{T,mean}$ е средната стойност на Wavelet енергията на некомпрометирани състояния и $E_{T,lim}$ е толерансният лимит на $E_{T,i}$.

Стъпките на алгоритъма са описани по-долу:

Стъпка 1: За всяко от множеството некомпрометирани състояния на IoT устройството се изчислява и запаметява $E_{T,i}$ (i=1,…,n).

Стъпка 2: Изчислява се:

$$E_{T,mean} = \frac{1}{n}\sum_{i=1}^{n} E_{T,i} \qquad (2)$$

Стъпка 3: Изчислява се $E_{T,lim} = k \times E_{T,mean}$

Стъпка 4: След всеки цикъл на работа (измерване) t на системния монитор:

- Измерва се и запаметява $E_{T,t}$

- Ако $|E_{T,mean} - E_{T,t}| > E_{T,lim}$, то състоянието на устройството се приема за компрометирано .

Стойността на $E_{T,lim}$ е избрана да е равна на $k \times E_{T,mean}$ (Стъпка 3), за да се вземат под внимание вариациите на натоварването на паметта на IoT устройството при различни компрометирани състояния и неточностите при измерването от системния монитор. Трябва да се отбележи, че тази стойност оказва влияние върху откриваемостта на компрометирани състояния и

следва да се избере евристично, на базата на предишен опит и/или литературните източници [3, 4].

3. ЕКСПЕРИМЕНТ

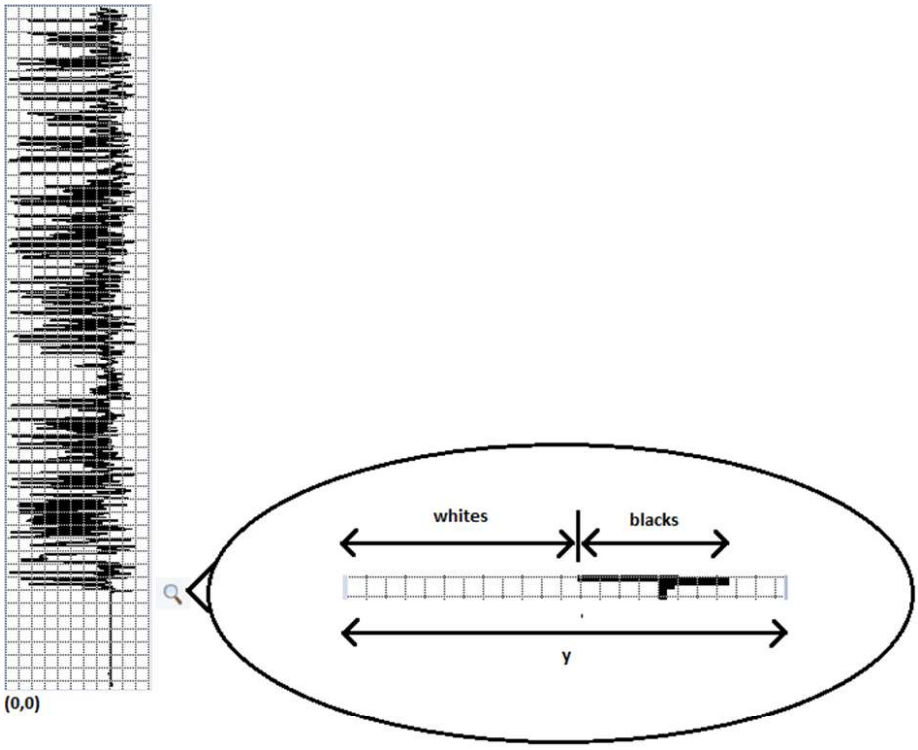
С цел да се сравнят експерименталните резултати със съществуващи подобни реализации на системи за идентифициране на различни компрометирани състояния на IoT устройства тук са използвани изходните данни от [4] за натоварването на паметта на IoT устройството, в проценти (Не е реализирана стъпка 1 на алгоритъма, тъй като IoT полигона, включително системата за мониторинг са в процес на разработване и/или доставяне на IoT устройства и мрежово оборудване) .

За целта първо чрез Snipping Tool са взети (без самите абсциса и ордината) графиките за натоварването на паметта на IoT устройството, в случаите, когато е некомпрометирано [4, фиг. 2] и когато е компрометирано (вследствие на SQL Injection) и реализира филтрация по предварително зададено поле на таблицата[4, фиг. 3].

След това всяка от фигурите се обработва чрез графичния редактор Paint. Обработката цели получаването на bmp файл, съдържащ само бели и черни пиксели, като началото на координатната система е разположена най-долу най-ляво на изображението и включва следните етапи:

- Rotate 90º;
- Flip Horizontal;
- Resize;
- Save as...

На фиг. 1 са показани основни моменти от преобразуване на изображенията.



фиг.1 Обработка на изображение в графичния редактор Paint.

```
import os
import platform
import pandas as pd
import pywt
```

```
cwd = os.getcwd()
df = pd.read_csv(cwd + "/EMO-Calculated/Square/Pr3.csv")
testValues = df['Value'].to_list()
cA , cD = pywt.dwt(testValues, 'haar')
sum = 0

for i in range(0, len(cA)):
    sum = sum + pow((cA[i]*100),2)

print(sum)
```

фиг.2 Python скрипт за предложения алгоритъм.

След това всеки от тези bmp файлове [8] се обработва чрез авторска приложна програма написана на C. В резултат на обработката се получава текстов файл с толкова редове колкото има изображението в bmp файла. Форматът на bmp файла включва header с описание на структурата и размера на изображението, последван от кодовете на пикселите в редовете на изображението (кодовете на пикселите в първия ред се изобразяват най-долу в изображението). Данните се прехвърлят в таблицата на Excel, като всеки ред от таблицата съдържа съответно броя (започвайки от абсцисата) бели и броя на последващите ги черни пиксели в изображението. След това данните се обработват като се записва индекса за използването на паметта, т.е. усреднената стойност в относителни единици, (брой бели пиксели + ½ от броя черни пиксели)/брой пиксели по абсцисата в изображението, (Вж. дясната част от фиг. 1).

Накрая, данните във всяка таблица на Excel (относителните единици) се мащабират към (ординатата) процентите на натоварването на паметта на IoT устройството [4].

Така от графиките в [4] се получават в табличен вид изходните данни за провеждане на експеримента.

Поради ограничения обем на работата в github [6] са дадени предложената програма на C и получените bmp и excel файлове (данните са представени графично и таблично) за натоварването на паметта на IoT устройството, в случаите, когато е некомпрометирано и когато е компрометирано.

Разработен е авторски скрипт на Python, основната част на който е показана на фиг. 2. В скрипта се извиква библиотечната функция ***pywt.dwt (testValues, 'haar')***, пресмята се сумата от квадратите на коефициентите на тенденцията (елементите в масива ***cA*** от тип ***numpy.ndarray***) и така изчислената стойност за енергията- E се отпечатва.

Резултатите от работата на Python скрипта върху данните за натоварването на паметта на IoT устройството, в случаите, когато е некомпрометирано, и когато е компрометирано са показани в табл. 1.

табл. 1. Резултати за натоварването на паметта

	E
Некомпрометирано	315904.4
Компрометирано	343753.5
Разлика в енергията	8.8 %

В първия ред е дадена енергията E за натоварването на паметта на некомпрометираното IoT устройство, във втория ред - енергията E за компрометираното IoT устройство, а в третия ред- разликата в проценти между енергията E за компрометираното и некомпрометираното състояние.

табл. 2. Резултати за натоварването на процесора

	E
Некомпрометирано	210209.9
Компрометирано	203995.6
Разлика в енергията	-3.0 %

табл. 3. Резултати за натоварването на мрежовия порт

	E
Некомпрометирано	55775.2
Компрометирано	53406.4

Разлика в енергията	4,2 %

Получените резултати за натоварването на процесора и мрежовия интерфейс на не/компрометирано IoT устройство, съответно са показани в табл. 2 и табл. 3.

От сравняването на получените резултати използвайки индексите за натоварването на паметта (табл. 1), процесора (табл. 2) и мрежовия интерфейс (табл. 3) се вижда, че най- голяма е разликата между енергията E за компрометираното и некомпрометираното състояние на устройството при натоварването на паметта ΔE =8.8 %. Това напълно съответства на резултатите и изводите от [4], което е вид верификация на получените тук резултати. От друга страна, целесъобразно е стойността на k да се избере равна на 0.08 (стъпка 3), т.е. малко под ΔE =8.8 % (табл. 1), за да се вземат под внимание вариациите на натоварването на паметта на IoT устройството при различни компрометирани състояния и неточностите при мониторинга.

5. ЗАКЛЮЧЕНИЕ

Предложена е система за детектиране на компрометирани IoT устройства в резултат на кибератака използваща Wavelet трансформация на Haar върху индексите за натоварване на паметта записвани от системния монитор. Резултатите получени в настоящата работа се очаква да намерят приложение в инженерната практика, както и могат да бъдат внедрени в процеса на обучение във ФКСТ на Технически университет София, където авторът е докторант.

Предстои допълнителна работа, свързана с изследване на приложимостта на разработените модели в киберсигурността на Интернет на нещата и по-точно идентифициране на компрометирани IoT устройства (в резултат на кибератака) на базата на анализ на методите и средствата на системите с изкуствен интелект чрез мониторинг на използването на процесора, паметта и мрежовия им комуникационен интерфейс. Предстоящата работа включва следните етапи:

- Разработване на хардуерна реализация върху FPGA на системата за детектиране на компрометирани IoT устройства в резултат на кибератака;
- Разработване на програмната част на системата за мониторинг на натоварването на паметта на устройствата в IoT полигона;
- Уточняване на параметрите на системата за идентифициране на компрометирани IoT устройства в резултат на кибератака;
- Верификация и валидация чрез измерване и/или сравняване с резултатите от известни такива модели.

Благодарности

Изследванията, отразени в настоящата статия са финансирани от НИС към ТУ-София по договор 212ПД00001-09

Литература

1. Hristov, A., Trifonov R. An application for temperature monitoring of integrated circuits of bitcoin miners, CAx Technologies Journal, issuue No 7, December 2019, ISSN 1314-9628, pp. 19-24.

2. Trifonov, R., et. al. Network and Information Security, Avangard Prima, 2013, ISSN 978-619-160-183-7 (in Bulgarian).

3. Hristov, V., REMOTE CONTRL OF DEVICES TROUGH SSH TUNNEL, Bulgarian Journal for Engineering Design, issue 38, January 2019, ISSN 1313-7530, pp.21-26

4. Sukhoparov M., Lebedev I. Identification the Information Security Status for the Internet of Things Devices in Information and Telecommunication Systems. Systems of Control, Communication and Security, 2020, no. 3, pp. 252-268 (in Russian).

5. Tan L., Jiang J. Digital Signal Processing 2nd Edition, Academic Press, ISBN: 9780124158931, 2013

6. https://github.com/sashkinaaa/readValuesFromBMP Посетен на 19.04.2021г.

7. https://github.com/sashkinaaa/Haar_1D_Filter/blob/main/pywt-haar1D.ipynb Посетен на 19.04.2021г.

8. https://api-2d3d-cad.com/bmp/ Посетен на 13.03.2021г.

INTELLIGENT SYSTEM FOR IDENTIFICATION OF COMPROMISED INTERNET OF THINGS DEVICES AFTER CYBERATTACK

Aleksandar HRISTOV
Department "Information technologies in industry", Technical University- Sofia, Bulgaria
e-mail: ahristov@tu-sofia.bg

Abstract: The purpose of present paper is to propose an intelligent system for identification of compromised Internet of Things (IoT) devices due to cyberattack, using Wavelet transformation and Haar filter. Monitoring is being made and the state is identified through time-synchronized series of indexes for usage of processor, memory and network port. Using system monitor the time-synchronized indexes of non-compromised IoT devices are saved as well as indexes of compromised IoT devices due to some well-known cyberattacks in Internet of Things are saved. The parameters of the proposed system are being specified in order to distinguish (filter) the two states of the IoT devices (non-compromised or compromised) by these indexes.

Keywords: Information Security, Artificial Intelligence Systems, Internet of Things, Wavelet transformation, IoT devices