A model for identification of compromised devices as a result of cyberattack on IoT devices

Aleksandar Hristov and Roumen Trifonov

Department “Information technologies in industry”

Faculty of Computer Systems and Technologies

Technical University of Sofia

ahristov@tu-sofia.bg, r_trifonov@tu-sofia.bg

Purpose of the paper

- The present paper aims to propose a 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 interface card
- 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

Relevance of the problem

- Nowadays information and communication technologies are becoming the basis of all our activities: economics, administration and private life
- The interest in the Internet of Things (IoT), the Industrial Internet of Things (IIoT) and in particular the information security [3] of IoT devices is constantly growing
- The review of the literature showed that the problem with information security of IoT devices is still poorly developed and there are no available systems for detecting compromised IoT devices as a result of cyberattack
- We believe that the results will be of national and international importance, considering the National Research Strategy and the challenges set out in it, as well as the institutional and European priorities

An universal method for identifying compromised states

- This method uses coefficients obtained from the Wavelet transformation for the memory usage (in percentage) of the IoT device
- The wavelet transform [5] is a transform that provides both time and frequency representation of a signal
- Decomposition: some portion of the signal, corresponding to some frequencies, is being removed from the signal
- The decomposition is repeated to a predefined decomposition level
- One subsignal is a running average or trend, T
- The other subsignal is a running difference or fluctuation, d

Algorithm

- The method for identifying of various compromised states of IoT devices uses as a metric the energy value of the Wavelet transform [5] for the memory usage
- This method is a two phase process. At the first phase (Initial Phase), the Wavelet energy value of non-compromised IoT device is measured and stored
- In the second phase (Test Phase) the Wavelet energy of the tested IoT device is measured and compared to the corresponding reference value
- The detection of a compromised IoT device will be successful when its Wavelet energy value exceeds certain tolerance limits.

Algorithm (2)

Given an initial set of n non-compromised states;

$E_{T,i}$ - the energy value of the memory usage of IoT device for different non-compromised states;

$E_{T,mean}$ - the mean Wavelet energy value of all non-compromised states;

$E_{T,lim}$ - the tolerance limit of $E_{T,i}$.

1. For each state from a set of n states of non-compromised IoT device is measured and stored $E_{T,i(i=1,\ldots,n)}$

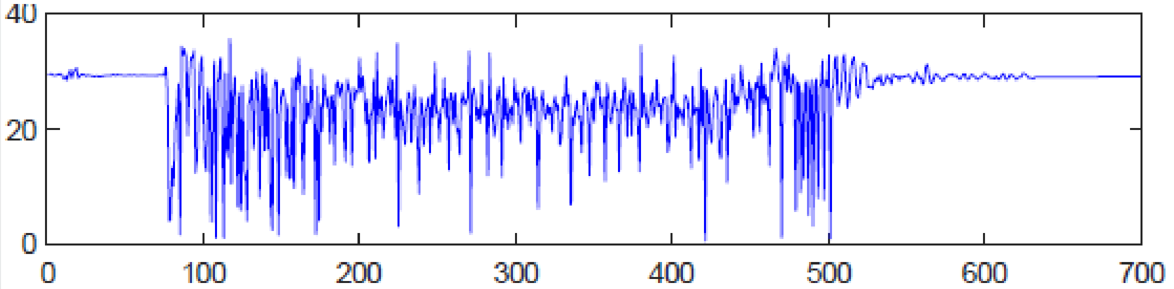
2. $E_{T,mean} = \frac{1}{n}\sum_{i=1}^{n} E_{T,i}$ is measured

3. $E_{T,lim} = k \times E_{T,mean}$ is measured

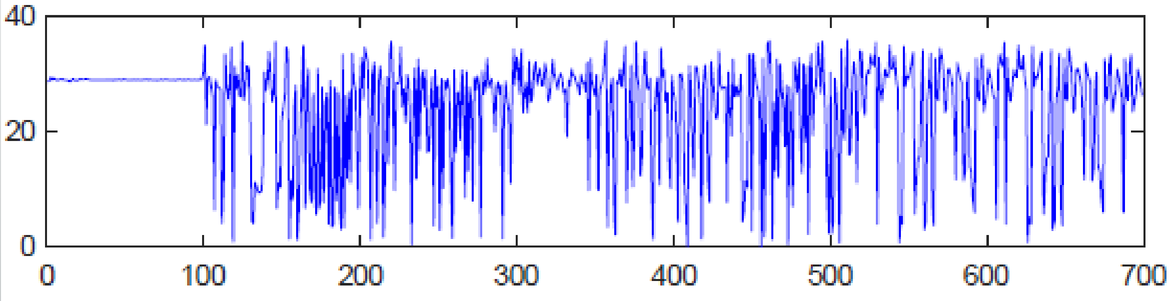
4. After each cycle of the system monitor t, $E_{T,t}$is measured and stored . If $|E_{T,mean} - E_{T,t}| > E_{T,lim}$ then declare as compromised the t state (using the energy value of current waveform)

Experiment

- In order to compare the experimental results with existing similar implementations of systems for identifying various compromised states of IoT devices, the initial data for the memory usage (in percentages) of the IoT device from [4] is used below
- For this purpose, screenshots of the figures from [4] for the memory usage of the IoT device are taken using MS Snipping Tool [4, fig. 2] and [4, fig. 3]



Compromised state



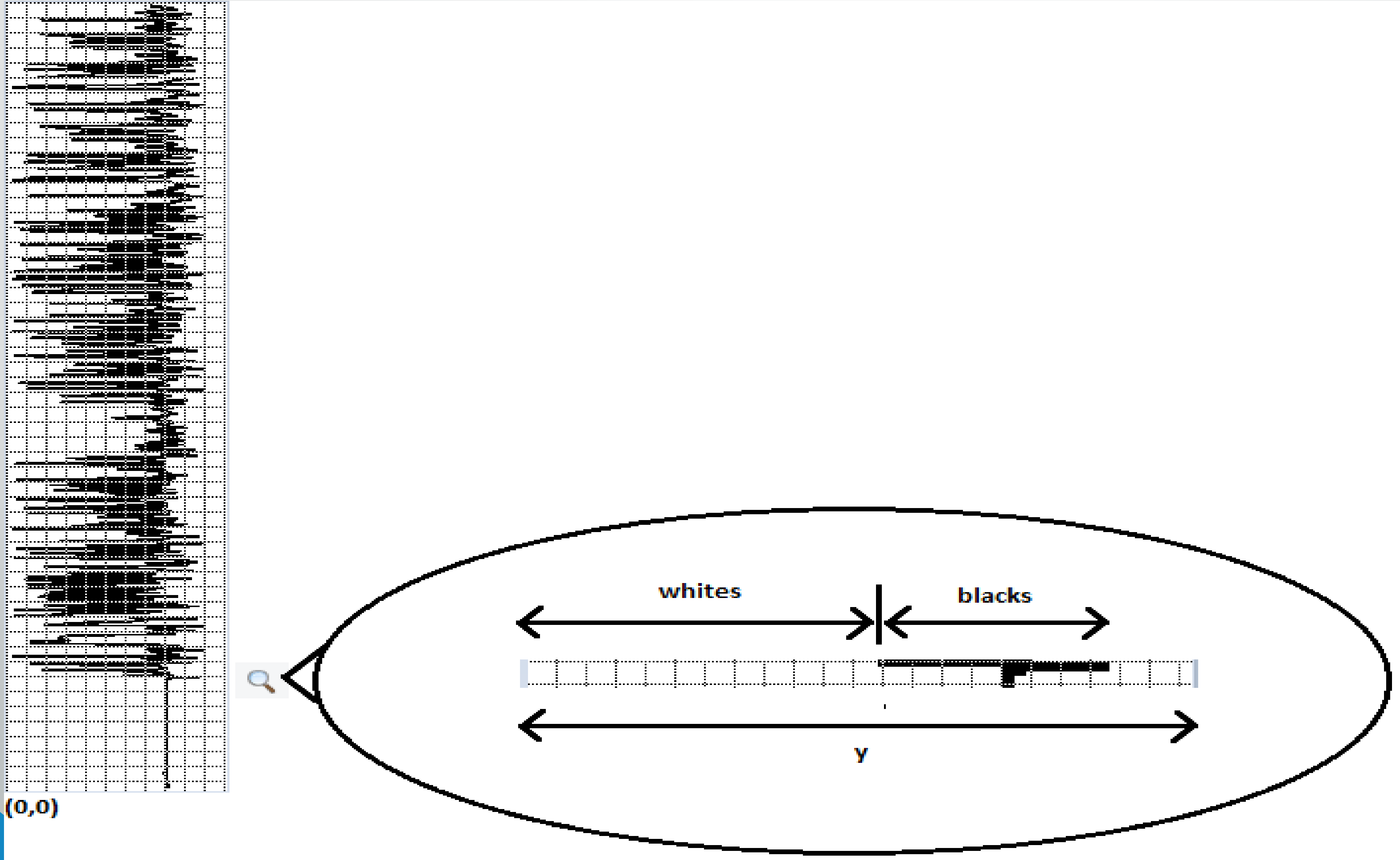
Non-compromised state

Experiment (2)

- For this purpose, screenshots of the figures from [4] for the memory usage of the IoT device are taken using MS Snipping Tool [4, fig. 2] and [4, fig. 3]
- Then each of the figures is processed using the graphics editor Paint. The purpose of the processing is to obtain a bmp file containing only white and black pixels with a size of 512x112 pixels
- Then each of the bmp files is processed by the author's application program written in C. The result of the processing is text file with as many rows as the bmp image contains
- The output data from the C program is transferred to an Excel spreadsheet. Each row of the spreadsheet contains the number (starting from the X-axis) of white pixels and the number of black pixels in the image
- The data is then processed and memory usage index, i.e. the average value (number of whites + ½ of the number of blacks) / number of pixels on the X-axis) in relative units is recorded

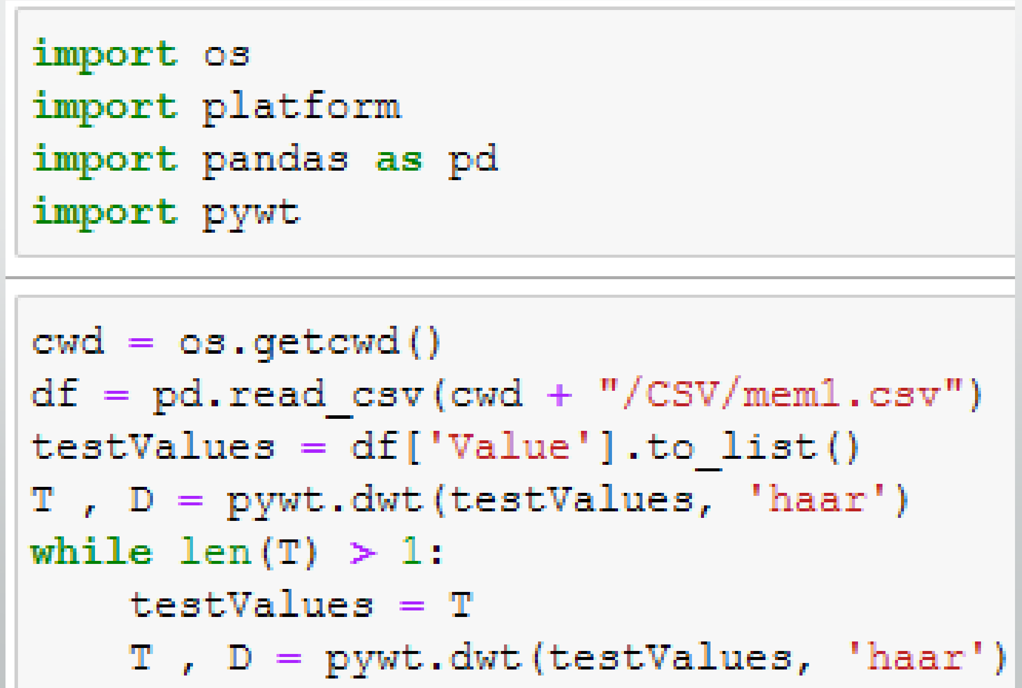
Experiment (3)

- Due to the limited size of the current paper in [7] are given the proposed program written in C and the output files from the processing: bmp and excel files (data is presented graphically and in tabular form)



Experiment (4)

- A Python script [8] has been written by the authors of the paper and the main part is shown in the fig below
- The purpose of the script is to calculate a single value for the trend, T. This is achieved by iteratively calling the function **dwt (x, 'haar')** from the module **pywt** to calculate the coefficients of the trend (for the first, second, …, eighth level of decomposition), taking into account only the trend coefficients of the previous decomposition level. The while loop stops when a single value for the trend, T is calculated, i.e. there is only one element in the array T, which type is **numpy.ndarray**
- The last obtained coefficient for the trend T is squared in order to calculate the energy, E



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

```python
cwd = os.getcwd()
df = pd.read_csv(cwd + "/CSV/mem1.csv")
testValues = df['Value'].to_list()
T , D = pywt.dwt(testValues, 'haar')
while len(T) > 1:
    testValues = T
    T , D = pywt.dwt(testValues, 'haar')
```

Results

- Results from the Python script execution on memory usage data of the IoT device are shown in the table
- The first row of the table shows the coefficient of trend, T and the energy, E for the memory usage of a non-compromised IoT device
- The second row shows the coefficient of trend, T and the energy, E for the memory usage of a compromised IoT device
- A third row is added to the table, in which the difference in percentages between the energy E for compromised and non-compromised state of the IoT device is given

	T	E
Non-compromised	539.2	290726
Compromised	567.3	321829
ΔE		**10.7 %**

Conclusion

- An intelligent system for identification of compromised IoT devices due to cyberattack, using Wavelet transformation and Haar filter for the indexes of memory usage has been proposed
- The results obtained in the present paper are expected to find application in engineering practice, and can be implemented in the education process at the Technical University of Sofia
- As a further work we plan to study the applicability of the developed model in the cybersecurity of the Internet of Things and identification of compromised IoT devices (as a result of cyberattack) more accurately. Improving accuracy in identification will be based on the methods of the artificial intelligence systems by monitoring the usage of the memory, CPU and network interface card

References

[1] Hristov, A, R. Trifonov, 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] Hristov, V., REMOTE CONTROL OF DEVICES TROUGH SSH TUNNEL, Bulgarian Journal for Engineering Design, issue 38, January 2019, ISSN 1313-7530, pp.21-26.

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

[4] Sukhoparov M. E., Lebedev I. S. 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., J. Jiang. Digital Signal Processing 2nd Edition, Academic Press, ISBN: 9780124158931, 2013.

[6] Zendara O., et. al. Swarm intelligence-based algorithms within IoT-based systems: A review

[7] https://github.com/sashkinaaa/readValuesFromBMP

[8] https://github.com/sashkinaaa/Haar_1D_Filter/blob/

main/pywt-haar1D.ipynb.

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/

NIST.SP.800-181.pdf

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6308658/

[11] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Thank you for your attention