REMIND
Some ideas for improved security for elderly

Eric Järpe, researcher ID 56, secondment 37

May 8, 2019

1 Introduction

During secondment 37, the following activities were conducted in Jaén, Spain:

- 2019-04-01 – 2019-04-05 Reading journal papers [1]–[31] related to study about early warning system of dementia.
- 2019-04-06 – 2019-04-07 Reading journal papers [22, 15] about security aspects of health care data.
- 2019-04-08 Suggestion to Mar Olmo, AgeingLab to collaborate about a study of dementia data for development of change-point detection methods for an early warning system of dementia indicators. This study would especially focus on how to properly take data into account from a care recipient's perspective, i.e. realize which variables are most relevant for being included in the model and correctly include mechanisms of how data are produced for being part of the method development.
- 2019-04-08 Suggestion to Mar Olmo, AgeingLab to collaborate about needs for development of security routines in treatment of health care data. This could mean confidentiality protection mechanisms, web form security for integrity guarantees when reporting sensitive data via a homepage, or int
- 2019-04-09 Completion of the research paper *Detecting change of activity intensity in smart homes* for submission to the Elsevier journal *Pervasive and Mobil Computing* in collaboration with colleagues Jens Lundström and Antanas Verikas.
- 2019-04-25 Meeting at the *Colombia Café 50* with Mar Olmo, AgeingLab.
- 2019-04-25 Visit to the care center *Angeles Cobo Lopez* in Alcaudete (residence of elderly people)

For the treatment of elderly people with smart health technology the accuracy and relevance of data is essential.

2 Objectives

The focus areas of this secondment were restricted from many perspectives.

2.1 Robust fall detection

An often discussed problem is the detection of falls, i.e. the falling to the floor of a patient [5]. Many elders are fragile and unstable and a fall can have devastating consequences. Falls are the sixth most common cause of death for people of 65 years of age or older [1]. A fall is a sudden event even though it can be a *slow fall* [10], i.e. occur slightly gradually by the patient fainting or, in the process of tripping on the floor, grabs an edge of a table or something to slow the fall to the ground. It is a tricky task to correctly recognize the falling of a patient in and it may be urgent in order to be save people from great suffering and to react at all to prevent them from dying.

To correctly recognize a person falling on the floor video cameras could be used [5] and this kind of data could make a great and revealing ground for proper recognition of falls. However, even though being an accurate and reliable medium for this kind of data, video cameras are, apart from being expensive and fragile, among the most integrity infringing sources of data. There is a clash of interests in, on one hand, the desire to have data which is accurate and relevant and, on the other hand, demands of the care recipient's integrity.

Less integrity conflicting data sources could be PIR or radar sensor which are mounted fixed in the smart home [19]. However, the cost for many sensors in the homes would be high and the possibility to correctly recognize falls by such means is weak.

Electricity consumption data has also been suggested as a less integrity conflicting means for activity data [16, 12]. This the additional advantage of being data that already "exists" – no extra hardware have to be installed in order to make observations from this channel. Again, as for the PIR and radar sensors, the accuracy for fall detection would be weak and long delay of alarm could be expected.

Wristbands and smart bracelets have proved a successful solution [30, 18] though they are not cheap. Still, progress has been made, e.g. by using low cost algorithms so that the device can be less expensive [26]. The snag here is that all these wearables need recharging, which is sometimes neglected, and annoyance from wearing the devices has commonly led to care recipients laying them aside – and if the device battery has run out or if it is not worn at all, the detection of the fall can have disastrous consequences. Accelerometers are also usually less good in detecting slow falls. In addition, more advanced solutions, such as with robotics [20] have been suggested.

A suggestion for dealing with this challenge with a more robust solution. One that combines the accuracy from the wristbands with the unremitting delivery of the PIR sensors and still not be as integrity intrusive as video cameras. To this end a combination of different sources is suggested. A study with this purpose could be designed with observations from a few PIR sensors, energy consumption logs, and a cheap smart bracelet which could be considered as better integrity preserving than video cameras. Then a comparison of some measure of how well these sources are able to detect falls (and possibly other urgent events) could be carried out. Possibly a combination of, say, just a few PIR sensors, a simple smart bracelet and energy consumption data could be evaluated for the purpose of more accurately detecting falls and anomalies in a less integrity infringing way. To this end, patients would have to be observed with many kinds of data sources during a long period in order to include observations of falls (and possibly other events) to act as ground truth. In the analysis of data, one could consider just the data coming from the PIR sensors, say, compared to the just the data from the smart bracelet and so on for the comparison. For the patients there would be no patients being solely observed by just PIR sensors of course, so there should be no ethical problem in the sense that there are patients who are not being considered from all the possible sources of data in order to react to events that call for urgent attention.

2.2 Victims of scams and financial exploitation

Another problem for patients suffering from different conditions, especially cognitive impairment ranging from Mild Cognitive Impairment (MCI) to Dementia (D) of different kinds, is their vulnerability to be victims of financial scams and attempts to profit on their reduced ability to protect themselves from these kinds of abuses [4, 29, 21, 2, 17, 11] even though the impression that elderly are not dominant among scam victims as opposed to younger generations has been claimed by [25]. A recent investigative report states that United States seniors lose at least 2.9 billion dollars from financial exploitation and consumer fraud [6]. In this report it is also conjectured that "Getting scammed could be and early sign of Dementia". Further, the Government Accountability Office of the USA found that around 14.1% of persons 60 years of age or older had experienced some kind of abuse, neglect or financial exploitation in the year 2011 [21].

An attempt in the direction of defining the concept of *Elder Abuse* has been made by the American authority *National Center on Elder Abuse*[1]. According to them, this abuse can be physical, sexual, neglective, financial, emotional or self-neglective. Financial abuse is further specified "misappropriation of a person's money or property" and warning signals of it are "Uncharacteristic purchases by the individual or caregiver; failure to pay bills or keep appointments; questionable behavior". They claim that Dementia and cognitive impairment are prime risk factors making older adults vulnerable to abuse and recommend contact with an Adult Protective Services agency or a long term care ombudsman. The term *Financial exploitation* was also given some attention by [8] and the American authority National Center on Elder Abuse [31]. The former included resources developed to help victims are a practice guide for attorneys specifically for all states of the USA, a compendium with documentation about cases

[1] URL: `https://ncea.acl.gov` and `https://ncea.acl.gov/FAQ.aspx`.

of abuse and an "elder justice toolkit", a collection of forms, tips and other tools. A great deal of definitions, aspects and ideas concerned with financial exploitation are found in the latter.

Today a common procedure for the administration of the more or less necessary private economy matters (like paying bills, internet shopping, borrowing books from the library, ordering tickets etc.) has become a standard routine for many people in all generations of adults. One of the difficulties for patients in early stages of dementia is the use of internet in order to pay bills and maintain contact with their bank. For the patients in early stages of cognitive impairment still living entirely independently this administration is an important issue. Also, it has been claimed that keeping up with maintaining business independently can help people in early stages of Mild Cognitive Impairment (MCI) or Dementia (D) to postpone their symptoms and have a longer and healthier life [14]. However, financial fraud is particularly damaging to the elderly as compared to other groups of the society [3, 7, 11, 9] which is why efforts to hinder such crime is strongly desired.

An idea for dealing with these problems could be to use artificial intelligence (AI) technology to guide patients using internet for their private economy (and maybe for other uses) and helping them in recognizing threats and keeping them on the track in their errands on the internet. Such a project could consist of the following steps:

- collection of data reflecting the success and problems of patients using the internet for these mentioned kinds of purposes or alternatively using data from another study of this kind
- development of a prototype of a guide based on the data from the investigation in the previous step
- observation of data from patients using the guide
- analysis of the data from both previous steps which includes the evaluation of how successful the performance of the guide is in protecting the patients from scams and, possibly, other benefits

Some steps in these directions will be indicated in this report.

3 Method

The long-term goal of this study is the quick and accurate detection of anomalies of different kinds. This chapter concerns with method aspects and these comprise essentially of two parts: treatment of data in preparation for change-point detection, possibly a machine learning step to further change multivariate complex data into univariate to feed to the change-point detection algorithms, and a change-point detection step which entirely deals with the complex data from the initial preprocessing step or with data from the machine learning step.

3.1 Preprocessing of data

Observations of the variables chosen are made. These variables may be on an individual level and along with the values of each variable is the time registered. Examples of variables could be *Diagnose of patient* (values being: no cognition impairment – NCI, mild cognitive impairment – MCI, moderate cognitive impairment – CI or dementia – D), *Patient is using the internet* (values: yes or no), *Patient receives an email* (values: yes or no), *Patient receives a text message – SMS* (values: yes or no), *Patient receives a telephone call* (values: yes or no), *Patient receives a visit* (values: yes or no), *Patient has been a victim of financial exploitation before* (values: yes or no) etc.

Sometimes observations of variables need to be preprocessed in order to correspond to the conditions assumed for use in a model making a foundation for further analysis and results. In the case when the purpose is to detect an anomaly of some sort this may be done by observing data which is shifting as the anomaly occurs. Now, it may be that the variable under observation is subject to seasonal or nocturnal variation or affected by other variables which are dependent of the observation variable but independent of the anomaly to be detected. These other variables affecting the values of the observations of the variable of interest are called nuisance variables. Effect of nuisance variables may have to be separated from the variables reflecting the occurrence of an anomaly in order for this to be detected with some reasonable accuracy.

Example 1 *To illustrate the concept of nuisance variables, let us consider an example of another altogether different application.*

Suppose we want to detect the anomaly that there is a nuclear incident where nuclear radiation is leaking from a nuclear plant [13]. For this purpose we make observations of radiation levels X measured and times $t_1, t_2, t_3, \ldots$ yielding readings $X_1, X_2, X_3, \ldots$ at these time-points. So the anomaly to be detected is the shift of a nuclear plant starting to leak radiation at some time-point, and the observation process is a sequence of readings of radiation levels. Thus we would like to develop a method which indicates if a sudden systematic increment of the radiation levels occur.

However, if this study would be performed in Sweden, a layer of snow would be likely to be present in the winter at many places. Since the radiation levels at times when there is no leakage would be observations of the harmless background radiation from the ground, the levels would be lower at winter time and there would be a dramatic shift to higher (but still harmless) levels every spring as the snow melts away. Therefore, to improve the properties of a radiation warning system based on these data, the radiation data should be "cleaned" from the effect of snow precipitation prior to be subject to the change-point detection stopping rule. Most commonly this would be performed by deploying a regression model and keep the residuals once having explained the seasonal affect of the response radiation *by the covariate* snow precipitation *or* snow depth *(see [13] for explicit details about this procedure).*

3.2 p-value estimation

This step requires a metric for measuring the distance between observations. That is, for N observations, there is a symmetric square matrix

$$D = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1N} \\ d_{21} & d_{22} & \cdots & d_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ d_{N1} & d_{N2} & \cdots & d_{NN} \end{pmatrix}$$

where d_{ij} denotes the distance (according to some metric) between observation i and observation j.

A very simple and intuitive algorithm is the *most central pattern* (MCP). It builds on the observation that if one uses the Euclidean distance metric then the sample that is most central, i.e. closest to the mean of all the samples, will be the sample that has the minimum row sum in the distance matrix D. The same of course holds for an elliptic Gaussian and using a corresponding Mahalanobis metric.

The MCP algorithm selects the pattern in the training set with the minimum row sum in the distance matrix (1) and uses this as the central sample. The set of distances from the remaining samples to this sample are then used as the empirical distribution (the "training set"). The p-value for a test sample m is then estimated as the number of samples in the training set that lie further away from the central sample The histograms are normalized so that the sum over bin counts equals one.

3.3 Change-point detection

Assume that a sample, $\{\epsilon_s\}_1^t$ of the random process $\{\varepsilon_s\}$ is observed. Then the likelihood function, $L(\lambda) = f(\epsilon_1, \epsilon_2, \ldots, \epsilon_t; \lambda)$, is the value of the joint density function of the variables $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_t$ as a function of the parameter(s). The **likelihood ratio**, $\frac{f(\epsilon_1,\epsilon_2,\ldots,\epsilon_t;\lambda_1)}{f(\epsilon_1,\epsilon_2,\ldots,\epsilon_t;\lambda_0)}$, is sufficient for inference about λ. Let θ be the change-point (a random time-point) and

$$\varepsilon_t \overset{\mathcal{D}}{=} \begin{cases} f_0(\epsilon_t) & \text{for } t < \theta \quad \text{in-control} \\ f_1(\epsilon_t) & \text{for } t \geq \theta \quad \text{out-of-control} \end{cases} \tag{1}$$

for all $t \in \mathbb{Z}^+$ where f_0 and f_1 denote marginal density functions of ε_t. The change-point problem is to detect the change-point θ as quickly and as accurately as possible, by just observing the process $\varepsilon = \{\varepsilon_t : t \in \mathbb{Z}^+\}$.

Here, the variables are residuals from the preprocessing of p-value estimates from the machine learning step. Assuming that this is just a sequence of p-value estimates without seasonal or nocturnal effects, the support for the distribution of these variables is the interval $[0, 1]$ and the the distribution, under ideal circumstances, is $U(0, 1)$, the uniform distribution on this interval. Thus the in-control density, referred to as f_0 in Equation (1), is the uniform while the out-of-control one, referred to by f_1 above, is one that is trending towards 0. One choice for the out-of-control distribution could be a triangular distribution, also with support $[0, 1]$ but skewed to 0 as would be

$$f(\epsilon_t) \;=\; (1 - \epsilon_t) I(\epsilon_t \in [0, 1])$$

where $I(\cdot)$ is the *indicator function* attaining the value 1 whenever the argument is true and 0 otherwise.

Now, for the change-point detection methods to work properly it is convenient if the process in-control has expectation 0. Therefore the simple shift from $[0, 1]$ to $[-0.5, 0.5]$ is suggested. This means the simple translation

$$X_t \;=\; \varepsilon - 0.5$$

for all $t \in \mathbb{Z}^+$ of the random variables and correspondingly $x_t = \epsilon_t - 0.5$). This leaves us with the change-point problem, as defined in Equation (1), of detecting the change-point θ as soon as the distribution of the process variable X_t has shifted from distribution F_0 (corresponding to density function $f_0(x_t) = I(x_t \in [-0.5, 0.5])$) to distribution F_1 (corresponding to density function $f_1(x_t) = (0.5 - x_t) I(x_t \in [-0.5, 0.5])$).

Then a *change-point detection method* is a stopping rule which may be formulated

$$\tau \;=\; \inf\{t : a(X_1, X_2, \ldots, X_t) > C\}$$

where a is called *alarm function* and C is a threshold value. Some classical examples of change-point detection methods may then be defined by specifying their respective alarm functions. Denoting $a(X_1, X_2, \ldots, X_t)$ by a_t for short, the Shewhart [27] method would simply be defined with

$$a_t = X_t.$$

For the cumulative sum (CUSUM or Page) [23] method

$$a_t = \max_{1 \le s \le t} \sum_{u=s}^{t} \log(0.5 - X_u),$$

while for the Shiryaev[28] method

$$a_t = \sum_{s=1}^{t} \prod_{u=s}^{t} (0.5 - X_u)$$

and for the exponentially weighted moving average (EWMA or Roberts) [24] method

$$a_t = \sum_{s=1}^{t} (1 - \lambda)^{t-s} (0.5 - X_s)$$

assuming that there is no time-dependence between the variables of the process.

The properties of the different change-point detection methods can then be evaluated in terms of many performance measures such as *average in-control run-length* $ARL^0 = E(\tau \,|\, \tau < \theta)$, *probability of false alarm* $P(\tau < \theta)$, *average out-of-control run-length* $ARL^1 = E(\tau \,|\, \theta = 0)$, *expected delay of motivated alarm* $ED(\nu) = E(\tau - \theta \,|\, \tau \geq \theta)$ where the assumption $\theta \in Geo(\nu)$ is the most common, *conditional expected delay* $CED(t) = D(\tau - \theta \,|\, \tau \geq \theta = t)$, *probability of motivated alarm* $P(\tau = t \,|\, \theta = 1)$, *probability of successful detection* $PSD(d, \nu) = P(\tau - \theta \leq d \,|\, \tau \geq \theta)$, *predictive value* $PV(t, \nu) = P(\theta \leq t \,|\, \tau = t)$, and *stationary average delaytime* $SADT = \lim_{t \to \infty} E(\tau_1 + \ldots + \tau_{N+1} - t)$ where $\tau_1 + \ldots + \tau_N < \theta \leq \tau_1 + \ldots + \tau_N + \tau_{N+1}$. The classical methods have then been proven optimal in respect of these and other performance measures.

4 Conclusion

4.1 Multiple data sources for robust fall detection

A first step for development of a robust fall detection procedure would be to figure out how to define the machine learning step in order for all feeds from different data sources (PIR sensors, simple accelerometer, electric usage data logs, etc.) combined in a balanced way, result in a sequence of uniformly distributed p-value estimates.

Following steps would be to just implement the change-point detection methods suggested previously, and evaluation according to the aferomentioned performance measures. Examples based on real data would finally serve as confirmation of the validity of the developed procedures. Observe that for this evaluation of the procedures it is crucial to have ground truth about the data, i.e. information about when the actual falls occurred.

4.2 A guide for protection against financial exploitation

Here the steps would be the following:

- Collection of data reflecting the success and problems of patients using the internet for these mentioned kinds of purposes or alternatively using data from another study of this kind.
- Development of a prototype of a guide based on the data from the investigation in the previous step.
- Observation of data from patients using the guide.
- Analysis of the data from both previous steps which includes the evaluation of how successful the performance of the guide is in protecting the patients from scams and, possibly, other benefits.

Also here the evaluation could be made by determining the performance measures from a simulation study. And also here the paper would benefit by ending with an example of how the guide works as demonstrated on the real data observed.

References

[1] S. Abbate, M. Avvenuti, P. Corsini, J. Light, and A. Vecchio. Monitoring of human movements for fall detection and activities recognition in elderly care using wireless sensor network: a survey. In Y.K. Tan, editor, *Wireless Sensor Networks: Application – Centric Design*, chapter 1, pages 1–20. IntechOpen, 2010.

[2] NHS Digital Adult Social Care statistics. Safeguarding adults annual report, england 2015-16 experimental statistics. Technical report, Health and Social Care Information Centre, October 2016. Responsible statisticians: Leat, F. and Thickins, L.

[3] M. Button and C. Cross. *Cyber Frauds, Scams and their Victims.* Taylor & Francis, 2017.

[4] C. Carcach, A. Graycar, and G. Muscat. *The Victimisation of Older Australians*, pages 1–6. Trends and Issues in Crime and Criminal Justice, No 212. Australian Institute of Criminology, 2001.

[5] K. de Miguel, A. Brunete, M. Hernando, and E. Gambao. Home camera-based fall detection system for the elderly. *Sensors*, 17(12):1–21, 2017.

[6] C. Elton. The fleecing of america's elderly. *Consumers Digest*, November 2012.

[7] L.A. Fenge and S. Lee. Understanding the risks of financial scams as part of elder abuse prevention. *British Journal of Social Work*, 48(4):906–923, 2018.

[8] S. Galvan and J. Shaw. Tools for addressing elder financial exploitation in rural areas. Elder Justice Initiative Webinar, National Center on Law and Elder Rights, United States Justice Department of Justice, October 2018. URL: `https://vimeo.com/294251005`.

[9] B.E. Gavett, R. Zhao, S.E. John, C.A. Bussell, J.R. Roberts, and C. Yue. Phishing suspiciousness in older and younger adults: the role of executive functioning. *PLoS ONE*, 12(2):1–16, 2017.

[10] H. Gjoreski, M. Lustrek, and M. Gams. Context-based fall detection using inertial and location sensors. In de Ruyter B. Markopoulos P. Santoro C. van Loenen E. Luyten K. Paternè, F., editor, *Ambient Intelligence. AmI 2012. Lecture Notes in Computer Science*, volume 7683, pages 1–12. Springer, 2012.

[11] S.D. Han, P.A. Boyle, B.D. James, L. Yu, and D.A. Bennett. Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease*, 49(3):845–851, 2016.

[12] C.W. Ho, C.T. Chou, Y.C. Chien, and C.F. Lee. Unsupervised anomaly detection using light switches for smart nursing homes. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, pages 803–810. IEEE, August 2016.

[13] E. Järpe. Surveillance, environmental. In A.H. El-Shaarawi and W.W. Piegorsch, editors, *Encyclopedia of Environmetrics*, chapter 6. Environmental Policy and Regulation. Wiley, 2013.

[14] R.A. Judges, S.N. Gallant, L. Yang, and K. Lee. The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, 8(588):1–10, 2017.

[15] A. Kanev, A. Nasteka, C. Bessonova, D. Nevmerzhitsky, A. Silaev, A. Efremov, and K. Nikiforova. Anomaly detection in wireless sensor network of the "smart home" system. In *Proceedings of the 20th Conference of FRUCT Association*, pages 118–124. IEEE, 2017.

[16] K. Leong, C. Leung, C. Miao, and Y.C. Chen. Detection of anomalies in activity patterns of lone occupants from electricity usage data. In *2016 IEEE Congress on Evolutionary Computation (CEC)*, pages 1361–1369. IEEE, July 2016.

[17] J.C.M. Li, M. Yu, G.T.W. Wong, and R.M.H. Ngan. Understanding and preventing financial fraud against older citizens in chinese society: Results of a focus group study. *International Journal of Offender Therapy and Comparative Criminology*, 60(13):1509–1531, 2016.

[18] M.E. Longstreth, A. Slosser, R. Barry, K. Bovenzi, C. Carrico, and C. McKibbin. Older adults' intent to utilize apple watch-based fall detection technology. *Journal of the American Geriatrics Society*, 67:S294–S294, 2019.

[19] J. Lundström, E. Järpe, and A. Verikas. Detecting and exploring deviating behaviour of smart home residents. *Expert Systems with Applications*, 55:429–440, 2016.

[20] Mundher. A real-time fall detection system in elderly care using mobile robot and kinect sensor. *International Journal of Materials, Mechanisms and Manufacturing*, 2(2):133–138, 2014.

[21] Government Accountability Office. Stronger federal leadership could enhance national response to elder abuse. Report to the Chairman, Special Committee on Aging, U.S. Senate GAO-11-208, Government Accountability Office, March 2011.

[22] G. Pachauri and S. Sharma. Anomaly detection in medical wireless sensor networks using machine learning algorithms. In *4th International Conference on Eco-friendly Computing and Communication Systems*, volume 70, pages 325–333. Procedia Computer Science, Elsevier, 2015.

[23] E.S. Page. Continuous inspection schemes. *Biometrika*, 41:100–115, 1954.

[24] S.W. Roberts. Control chart tests based on geometric moving averages. *Technometrics*, 1(3):239–250, 1959.

[25] M. Ross, I. Grossman, and E. Schryer. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science*, 9(4):427–442, 2014.

[26] M. Saleh and R.L. Jeannes. Elderly fall detection using wearable sensors: A low cost highly accurate algorithm. *IEEE Sensors Journal*, 19(8):3156–3164, 2019.

[27] W.A. Shewart. Economic control of quality control. *The Bell System technical journal*, 9:364–389, 1930.

[28] A.N. Shiryaev. On optimum methods in quickest detection problems. *Theory of Probability and Its Applications*, 8(1):22–46, 1963.

[29] R.G. Smith and C. Budd. *Consumer fraud in Australia: costs, rates and awareness of the risks in 2008*, pages 1–6. Trends and Issues in Crime and Criminal Justice, No 382. Australian Institute of Criminology, 2009.

[30] P. van Thanh, D.T. Tran, D.C. Nguyen, N.D. Anh, D.N. Dinh, S. El-Rabaie, and K. Sandrasegaran. Development of a real-time, simple and high-accuracy fall detection system for elderly using 3-dof accelerometers. *Arabian Journal for Science and Engineering*, 44(4):3329–3342, 2019.

[31] S. Wood and P.A. Lichtenberg. Financial capacity and financial exploitation of older adults: Research findings, policy recommendations and clinical implications. *Clinical Gerontologist*, 40(1):3–13, 2017.