A new unsupervised learning-based process for extraction of knowledge’s and improving anomalies detection

A. Lasbahani, C. Taoussi
Laboratory RMI, University Hassan 1
Laboratory LIPIM, University sultan moulay slimane
abbdellatif.las@gmail.com

Abstract. Lately, the world confronts day by day the birth of typically big data in various fields such as health, telecom, electronic sales, communication, service provision, industry, e-learning and e-commerce. This emergence was a brick and a major reason behind the realization of immense changes in the processes of manipulation and processing of data as the system of storage, processing, analysis and visualization of data. From an application point of view, the manipulation of such data requires the implication of certain numbers of usage standards such as those related to security, credibility and optimization of data. However, it seems so difficult to ensure the security of massive and gigantic data coming from a variety of sources, and especially in real time, because there is an almost total absence of methodologies ensuring the processing and protection of a volume of data automatically. In fact, our work takes stock of a new process allowing the secure handling of big data. This is about getting more out of machine learning, security patterns and decision trees. More specifically, our approach aims to design machines able of securing large data in real time while making them learn from a mapping of security patterns (learning data). This training will allow machines to develop in terms of security, which will allow them to improve their intelligence related to the detection of anomalies caused in the data during the data exploitation operation.

1. Introduction

Currently, and given the amount of data transmitted over the internet, new technologies have emerged, which derive more fruit and results from the fields of mathematics, statistics and data processing. The objective behind these technologies is to put forward fundamental concepts to the manipulators of this data on the one hand, and to allow companies a better exploitation of the full data of productivity on the other hand.

However, several information’s circulating and transiting on the Internet from different sources. In addition, from which we will be able to create wealth in terms of scientific evolution, centralization of information, creation of new opportunities, improvement of productivity and sharpening of companies at the level of their center of interest. In addition, taking advantage of this data requires putting yourself in a number of practices, laws, rules of use and handling procedures. Several works have been suggested in this direction. More specifically, we find many contributions that acted to emphasize data preprocessing. This process represents the most essential phase requiring a higher awakening state, because there, where we perform deeper tasks in order to ultimately increase auspicious data; easy to understand and handle by machine.
Data cleaning is the process or operation, which consist to detect, remove and correct noise and inconsistent data that may affect the intended purpose as mentioned there. Then, after the validation of this process, we begin the integration phase which consists of merging data from different sources, which can be distributed databases not only sql or relational databases like [1]; we address the centralization of data in the heterogeneous databases called data warehouse [1]. These base stations can be connected to sensors, others databases, electronic instruments or any kind of equipment that can be identified by network address and connected to the Internet. On the other hand, several works have been proposed in this direction. Third, there is the selection phase, which consists of choosing the data that can provide new knowledge, as well as the data relevant to the analysis.

Before proceeding in the analysis phase, it is very important to go through the transformation phase whose objective is to transform the data structure in order to put them in a suitable format to activate the operation of (EDC) knowledge extraction; more precisely, we talk the reduction and aggregation tasks.

From an application point of view, several approaches, methodologies and algorithms have emerged dealing with knowledge extraction in general. Yet this field possesses in its entirety an enormous number of sub-domains, each of which has its own preoccupations and elementary tasks contributing to the overall process as matching scheme, data cleaning, data classification, Data analysis, background analysis and data visualization.

For example, if we account for the works given in the data-mining field, and based on the state of the art that we have brought, there is a variety of contributions, each of which breaks down into a more precise track. As described above, knowledge extraction requires a higher level of vigilance in terms of accuracy while reducing data loss on the one hand, and provide high performance data to the machine so that it can properly govern its context on the other hand.

However, based on the classification of these approaches based on a set of comparison criteria, we have concluded by agreement that the majority of these methodologies have several technical, organizational and strategic disadvantages, application and economic. When we present the economic difficulties and disadvantages, we aim at the price of realization, the technical architecture and the technical prerequisites of such tasks in relation to the results obtained. There is always a larger gap indicating that the internal structure of these processes requires an upgrade to meet our big data and data security needs.

The goal is to provide analysts, statisticians and leaders with solutions and strategies to ensure proximity and remark able forecasting while making the most of this volume of data. We are talking about the automation of certain data extraction and analysis tasks, as well as the power and the hypothesis to strengthen and why not to design new processes and process to ensure the semi-automatic automation of knowledge extraction by improving the level of criticality and security during data exchange and sharing.

We also try to learn from the difficulties and disadvantages of the existing work on the one hand, and to better adopt the research and techniques introduced in terms of artificial intelligence on the other hand. It should be noted that the processes of data processing and manipulation present to date have been able to benefit from the technological advances given in terms of machine learning, whether it be supervised learning, unsupervised learning, semi-automatic learning and deep learning and its variants. However, they fail to take into account the principle of versatility in terms of centralisation and automation of all data exploitation tasks including data security.

To this end, we intend to add a new deeper layer to this work in order to allow them to take into account the accuracy of data manipulation tasks including the ability to secure and validate data automatically in time real during the data manipulation process. The objective of this approach will be to design a new work-based data processing process. In addition, in this paradox, we will give researchers the opportunity to bring new results by focusing on the elementary parts of our process. It should be noted that our vision is to provide a standard of data processing that respects quality indicators such as portability, scalability, and recursion.
On the one hand, we aim in this work to take into account the conceptual structure of the data during the processing operation while establishing a strong link between the data processed during the commissioning of the computer solutions developed, thus also the modelling phase or the design phase. So it became easier and quite convenient to manipulate a large amount of data by living on the security side. The latter will be achieved by making the most of the safety bosses. These parts will be communicated in the form of data (dataset) from which we teach our system or machine the laws, the strategies, the mechanisms to incorporate to face vulnerabilities appearing during data processing.

2. Related works

Recently, various works have been done and designed to manipulate and ensure the scalability, sustainability and continuity of what scientific research has been able to achieve in terms of big data, more precisely; we are talking about tools, algorithms, Framework, platforms, workflows, software’s, hardware’s, models, programs, technical and statistical requirements. Before proceeding with the inventory of these contributions, we would like to take stock of big data. The last is a multidisciplinary field whose purpose is the processing and analysis of potentially large data referring to the following 3Vs: volume, variety, and velocity (frequency).

From a big data management point of view, a lot of work has been proposed to discuss the broad lines of all management. Big data management is a very active and moving field where analysts and scientists have faced several challenges to do and to measure in order to achieve the objectives identified during the birth of this field of science. Among these challenges we find the disciplines related to data collection, data storage, data integration and of course without forgetting the reduction of hardware and software requirements.

Other big data management challenges have been very successful, such as data reliability. This work focuses on data reduction, data aggregation, data mining, data encoding, and data security and protection. However, and given the calculations and statistics obtained in this direction, or in terms of detecting anomalies and enhancing the security of data from different distributed sources, there is only very little work such as [2], which were able to give new experiences with data extraction, data encoding, data evaluation and data security in one go. [2] emphasizes data security while referring to the principle of roles in order to design responsibilities on the one hand, and assignment of tasks on the other. On the other hand, this work does not have a documentary repository based on business standards that allows the development of detection data of all kinds of undesirable behaviour on test data, training and future data.

However, [3] has focused on security and access configuration using the RBA concept, which allows administrators to separate between different layers of the system. This involves assigning and organizing specific data according to role. Thus, these roles will be assigned to the entity concerned. Additionally, by collective agreement, this work suffers many disadvantages despite the fact that it had been able to overcome so many difficulties related to the control of access to data stored somewhere cluster, processing cluster, sensor and any other instrument. Among the challenges presented by this work, we focus on the lack of consideration of scalability, reliability, data flexibility, sustainability and data migration.

From a data centre perspective, the high-volume data security of a data centre [4] has been able to provide us with a deeper vision by securing business data through the management and structuring of role-based access profiles. Following our investigations and hypotheses, this work can draw more from the evolution that the backup systems have experienced in recent years, thus also to strengthen and develop in term protection of business data in a more particulate and adequate way to current needs.

Then all eyes turned to the new theorem presented in [5]. The latter had brought to the field of technological advances in terms of data security a new approach called Terminal Services and Xenapp Server Deployment whose purpose is allowing for better handling of multimedia through the session. However, this work does not have a comprehensive and deep vision of how to manage and to protect
data that previously had input errors, lacks integrity and compliance. In addition, it does not have a basis for decision making in the alternative case.

In addition, [6] presents a new contribution that focuses on Influences of architectural and implementation choices on Cyber infrastructure quality. In this work, authors offer a new concept based on the CYCORE’s CI, which uses the RS architectural pattern to separate application services from infrastructure services. However, this work was intended for the health field. So it cannot be generalized to other areas so that it is a basis for decisions in terms of security. So [7] was talented to discuss and present the principle of the Over blocking and under blocking allowing Content Filtering. On the other hand, this work suffers from many shortcomings such as the lack of precision regarding content filtering, the lack of a guide describing the strategy to be followed, etc.

More precisely, others works have been given to enhance security in social networks context that deal with big data. For example, we found [8], which present an incentive-based protection and recovery strategy for secure big data in social in which the users are divided into five states according to their reactions to data virus: susceptible, contagious, doubt, immune, and recoverable. Moreover, this work fails to describe on what basis generates their solutions desire to resolve attacks that may affect the user and his data.

In the context of big data, cloud computing and internet of things, several works have been proposed to secure the given flows. For example, we discuss [8], which monitors the Internet of Things and cloud computing technologies by focusing on the security issues that can be faced with these technologies. However, this work did not address performance specifics in the event of a change in context, system, platform, infrastructure, and use measures.

[9] Present a secure weighted possibility c-means algorithm based on the BGV encryption scheme is proposed for big data clustering on cloud. In the same context, [10] propose a secure big data deduplication with dynamic ownership management in cloud based on identity-based encryption and proxy re-encryption. However, this work does not take into account all the security properties during the development of the security scheme.

[11,12, 13, 14, 15] describes a new paradox whose objective is aiming to disclose the trust management techniques prevailing in IoT with a special focus on big data technologies, and will outline the new developments and approaches that are applicable in these areas.

Table 1. A comparison between the works given in this direction.

| Criteria                        | [6] | [7] | [8] | [9, 10, 11] |
|---------------------------------|-----|-----|-----|-------------|
| Degree of automation            | *   | *   | *   | *           |
| Type of methodology             | NF  | NF  | NF  | NF          |
| Integration phase and time      | NS  | NS  | NS  | NS          |
| Level of genericity and reuse   | *   | *   | *   | *           |
| Targeted security properties    | AC  | AC  | AC  | AC          |
| Methodological support          | N   | N   | N   | N           |

(*) : weak
(NF): No formal
As you notice, all the work presented so far suffers from the lack of automation of the entire data processing and protection process. They also require a very high and important level of experience for scientists and analysts, which lead to difficulties in manipulating such data. In addition to all this, all the contributions discussed in this sense do not have formal measures that allow them to be robust, scalable and sustainable. It should also be borne in mind that the levels of generosity of these works are still low compared to our solution. Finally, the majority of these works and even all of it cannot be standardized because of the lack of methodological support.

From this comparable study, it seemed to us that a new approach in this direction will be very interesting in order to take stock of the difficulties and the gap presented in the contributions given so far, and all this without diminishing the significant number of benefits brought, and the problems solved through this work.

In the next section, we present our paradox while focusing on the principle of how this approach works, as well as the benefits and gains that can be brought about by the reasonable application of this process.

3. Proposed approach

3.1. Overview of our process

In this section we present a general overview of our process which aims to increase a very high and moving level in terms of unsupervised learning, anomalies detection, data extraction, big data processing, standardization of data, standardization of the knowledge extraction process and reinforcement of the safety aspect, thus also, to put analysts and data science at the heart of the process of engineering gigantic data distributed in contexts led by cloud computing and the Internet of Things. To this end, we will see in detail the proposed methodology while putting all our efforts on the different parts of our approach including algorithms and tools.

Below we present the pre-processing phase of our process, which consists of mastering and enabling developers and architects to start the requirements and integrate security considerations on the one hand. In addition, to allow analysts to profile these results and fault detection rules used by these architects in order to cope with the data validation process by detecting all kinds of anomalies caused and committed during the commissioning of these data on the other hand.

More specifically, this phase is essential during the process of analysis and design, development or production, data storage, data distribution and data mining.

![Fig.1 : pre-processing phase of our process](image)

In this phase, we were able to propose the integration of this phase during the different phases of production and implementation of IT solutions in order to facilitate the creation of performance and wealth over time. To do this, during the modeling, architects are invited to integrate the consideration
of the security infrastructure by getting more out of the security patterns, and this in order to equip our data mining and processing process with intense and massive data to take stock of the detection of anomalies to do and as the process of storing and distributing data in different processing centers.

In other words, this link has become more crucial in the process of manipulating and exploring big data. Its purpose is to add a deeper layer to it in order to have structured data with data protection rules that comply with those imposed by security parties. It should be remembered that these patterns are scattered in a decision tree or pattern mapping. They connect with each other through links of inclusion, specialization, realization or collaboration. The fault detection data set is generated from this mapping by applying clustering or clustering algorithms such as k-means. The objective of this method is to specify the appropriate patterns according to the considerations.

Below we present the proposed algorithm in order to enrich and strengthen the process of data manipulation to understand the scenario of automation and protection of massive and intense data.

Algorithm 1 anomalies detection

Choose data set, security data set

Input:
Data set: \( ds \leftarrow \) structured data
Model of anomaly detection:
mad—Security patterns, decision tree, K-means

Data set: \( sdt \leftarrow \) security data set recover from the decision tree of security patterns

Output: a set of data a set of secure data, corrected and adapted to the negotiated security recommendations

\[
\text{while} \ ds \neq \emptyset \text{ and } sdt \neq \emptyset \{
\text{for each entite in } ds \
\quad \text{mad.map(entite, sdt)}
\}
\]

#anomalies detection

for each entite in \( ds \) {

if \( \text{entite.values().has_change()} \{
\quad \text{mad.detect_anomalies(entite)}
\quad \text{ent} \leftarrow \text{mad.get_statue_of_entitie_before_attack(entite)}
\quad \text{if ent} \neq \text{entite} \{
\quad \quad \text{noise} \leftarrow \text{mad.get_additional_section(entite)}
\quad \quad \text{solution} \leftarrow \text{mad.get_solution(noise, sdt)}
\quad \quad \text{mad.correct(entite, solution, sdt)}
\quad \quad \text{secured_data} \leftarrow \text{entite}
\quad \quad \text{else} \{
\quad \quad \text{secured_data} \leftarrow \text{entite}
\quad \quad \}
\quad \}
\}
\}

\text{return} \text{secured_data}

As you see above, the operating principle of our methodology is quite reasonable and easy to handle even for analysts and inexperienced scientists in data science and security. To this end, the idea is to enrich the modeling phase by taking into account the application of safety patterns. Practically, we will need two data sets, one of data (digital, symbolic, image, text, sound), and one of security (security patterns, security strategies, etc). This is how our algorithm works by matching these two
data sets. Then, and in real time, it scans the content of the data set by evaluating the representation and internal structuring of each entity of the data set, and this according to the security data set. Then there are two possible scenarios, if an entity has undergone drastic changes, our process will respond by detecting the additional part. Depending on the latter, the machine will promote the appropriate solution by correcting the faults caused. Then, the machine automatically attaches the contents of the original data set previously assigned to a new data set that is more secure and protected against all kinds of vulnerabilities. The second scenario, if the data set did not have attacks, the content will be reinforced by more relevant security solutions from the data set security patterns. Therefore, we will have a more relevant learning or prediction model with more developed and secure training data in accordance with the standards generated from the safety pattern shaft. In the same way, our model will be able to reason and make decisions easily, without having programmed it before, or to provide it with the desired results. Therefore, we just need to focus on the approach proposed in this work in order to obtain pleasant and incredible results. Below, we highlight the learning power of our strategy. Therefore, by making our machine learn by data processed according to our paradox, we were able to improve economic, strategic, material and intangible gains, and quality of services. More specifically, the loss rate is gradually decreasing, but the accuracy rate is always improving exceptionally.

In the next section, let’s see in detail the criteria of measures deployed by our approach to detect infected elements, and how to correct and strengthen them so as not to lose their integrity during all kinds of malicious uses by strange third parties.

3.2. Detection and correction of anomalies

In this section, we describe the flow chart of our algorithm to detect and correct fraud and all kinds of falsifications that can attack digital representations of data. For this purpose, as mentioned below, we begin by either developing a mapping scheme between the data set of our system’s data based on data and security data generated by experience from the security pattern tree. On this dataset, we find a collection or a series of experiments previously collected over time. In other words, the solutions generated to solve all kinds of vulnerabilities experienced on various types of data. This is how we perform an iterative process on the mapping result in order to get out all the noises still infecting the original data. This is why we browse this data set to analyze the current data set compared to the original. Then we collect the additional parts from each entity in our data set. Therefore, the correction will be made according to the solution generated automatically according to the noises appearing at the level of each entity. In the end, we will have a data set that is more efficient and able of dealing with malicious uses.
The algorithm below describes the details of the resolution of our problem in terms of correcting all kinds of lack of integrity at the real-time data level. First, we create a detailed data export context. Secondly, we evaluate the content of each element through the principle of modular and structured composition and decomposition. Thirdly, an upgrade is planned and adopted according to the falsifications committed. Finally, we recover a fully secure data set with as many performance requirements, protection and automatic real-time vulnerability remediation.

**Algorithm 2 anomalies improvement and correction**

**Input:**
- \(ds \leftarrow \) structured data, \(ds = \{d_0, d_1, d_2, \ldots \ldots, d_n\}\)
- \(sdt \leftarrow \) security patterns, security strategies, \(sdt = \{s_0, s_1, s_2, s_3, \ldots \ldots, s_n\}\)
- \(mdt \leftarrow \) mapping model, \(mdt = \{d_0^*s_0, d_1^*s_1, d_2^*s_2, \ldots \ldots, d_n^*s_n\}\)

**Output:**
- \(sds \leftarrow \) secured structured data, \(sds = (ds * sdt) / mdt\)

if (mapping \(ds\) regarding to \(sdt\) is achieved) and (\(mdt \neq null\)) {
  while (these has an element in \(mdt\)) {
    element = \(mdt\).getElement().next()
    noise = \(mdt\).getNoise(element)
    if \(noise \neq null\) {
      solution = \(mdt\).getSolution(noise)
      \(mdt\).correct(element, noise, solution)
      \(sds\).append(element)
    } else {
      \(mdt\).predict_solution_before_attack(element)
      \(sds\).append(element)
    }
  }
}

returns \(sds\)

4. Results

In this work, we plan to improve and facilitate the data processing phase while focusing on our scientific input. The latter has been able to overcome so many difficulties in data protection, and the
power to provide them with a specific layer of manipulation that will aim to increase data integrity, and ensure data reliability and robustness regardless of the attack mode that may occur during the activation of such data. For these purposes, we anticipated two problem-solving algorithms related to improving the detection of security anomalies on the one hand. In addition, provide an additional step to the old data processing process to integrate the security and automation aspects of data extraction. In other words, the former describes as reacting to strange elements. Moreover, the latter foresees as overcoming difficulties. Therefore, and as we see in the figures below, it will be possible to achieve great success by deploying these assumptions in a reasonable manner. Therefore, it is likely that the indicators will have desirable results. More specifically, we are progressing relatively from one iteration to another while increasing the level of performance in terms of security. We will have powerful machines capable of simulating intelligence in terms of safety learned unsupervised. It should also be noted that the integrity indicator is always evolving from one training to another.

5. Discussion
As you notice below Fig.6, we were able to isolate the part with unwanted combinations while keeping the integrity measures as shown on the red bubble as shown in figure Fig.5. We were also able to add the security strategies to the data after performing the data grouping using the k-means algorithm. More specifically, the data has colored blue, while the subsidies and performance improvement rules in terms of detection and correction of anomalies in green.
In addition, we were able to overcome the difficulties presented in previous work in terms of degree of automation, Type of methodology, Integration phase and time, Level of generosity and reuse, Targeted security properties, Taking into account the platform, Standardization of the approach and Methodological support.

6. Conclusion

In this work, we have proposed a new process of data manipulation while putting all our efforts on a well-defined engineering led by solutions already defined over time to resolve delicate situations related to the loss of big data, loss of semantics and meaning of data, difficulties in preparing data to value chain and lack of integrity. To do this, we began by defining the gaps and flaws that the field responsible for this kind of treatment suffers, and thus also identify all kinds of differences raised by all the work envisaged on this. It is also important not to forget the evolutionary criteria imposed by nature, which themselves had an important factor behind what we were able to achieve and do. To this end, we proposed a new data preparation methodology focusing on the aspect of detecting anomalies and correcting errors in real time. This practice has allowed us to profile the experiences previously stored at the level of safety patterns. These guidelines have been leaked as data and are dedicated to resolving vulnerabilities related to anomalies detected during data manipulation. In such a way, and by applying our strategies defined at the level of the algorithms negotiated, we will have the power and resources necessary to design the machines involved the field of artificial intelligence capable of preventing the future in terms of anomalies, thus also the ability to build real-time solutions to detected anomalies.

From an economic point of view, we will prevent a 50 percent reduction in expenses compared to previous work. It should be remembered that we will produce gains of up to 40 percent improvement over current statistics.

As perspectives, we plan to add other technical details such as the one related to fault tolerance, the automation of the whole chain of big data, take into consideration the data storage criteria and model a repository guiding the data scientist and analyst to perform similar tasks without having an important required level in terms of the subject matter.

References
[1] E. Rahm, H.H. Do, “Data cleaning: problems and current approaches”,IEEE Technology Bulletin on Data Engineering, Vol.23, No.4, pp.3-13, 2000.
[2] Cross, Michael, W. Thomas, Dr Shinder, “MCSA/MCSE 70-294: Active Directory Infrastructure Overview”,Vol. 70, pp. 1-81,2007.
[3] A. Hay,P. Giannoulis, K. Hay, W. Verbanec, “Nokia Firewall, VPN, and IPSO Configuration Guide: Security and Access Configuration”,Vol. 286, pp. 165-225,2009.
[4] [W. Gragido, J. Pirc, N. Selby, D. Molina, “Blackhatonomics: Drivers and Motives”,Vol. 59, pp. 35-43,2013
[5] T. Bin Azado, “Securing Citrix Presentation Server in the Enterprise: Terminal Services and XenApp Server Deployment”,Vol. 281, pp. 157-258,2008.
[6] E. Farcas, M. Menarini, C. Farcas, W. G.Griswold, K. Patrick, I. Krueger, B. Demchak, F.
Raab, Y. Yan, C. Ziftci, “Influences of architectural and implementation choices on CyberInfrastructure quality—a case study: in Software Quality Assurance”, Vol. 12, pp. 279-332, 2016.

[7] P. Nicoletti, CISSP, CISA, CCSK, “Content Filtering: in Computer and Information Security Handbook (Second Edition)”, Vol. 281, pp. e101-e122, 2013.

[8] Y. Wu, H. Huang, N. Wu, Y. Wang, M. Zakirul Alam Bhuiyan, T. Wang, “An incentive-based protection and recovery strategy for secure big data in social networks”, Information Sciences, Vol. 508, No. 1, pp. 79-91, 2020.

[9] C. L. Stergiou, A. P. Plageras, K. E. Psannis, B. B. Gupta, “Secure Machine Learning Scenario from Big Data in Cloud Computing via Internet of Things Network”, Handbook of Computer Networks and Cyber Security, Vol. 21, No. 1, pp. 525-554, 2020.

[10] Q. Zhang, Z. Chen, “A weighted kernel possibilistic c-means algorithm based on cloud computing for clustering big data”, International Journal of Communication Systems, Vol. 27, No. 09, pp. 1378-1391, 2014.

[11] S. Gonthireddy, S. Kumar Pasupuleti, “Secure Big Data Deduplication with Dynamic Ownership Management in Cloud Computing”, Advances in Intelligent Systems and Computing book series (AISC, volume 1089), Vol. 1089, No. 09, pp. 249-263, 2020.

[12] A. Lasbahani, M. Chhiba, A. Tabyaoui, O. Mjihil, Model Driven Architecture Approach for Application Security Integration, Journal of Theoretical and Applied Information, Vol. 95(8): 1655-1668, April, [On-line] 2017, Available.

[13] A. Lasbahani, M. Chhiba, O. Mjihil, Deals with integrating of security specifications during software design phase using MDA approach, Proceedings of the Second International Conference on Internet of things and Cloud Computing, Vol. 196, pp. 1-7, Cambridge, UK, March, 2017.

[14] A. Lasbahani, M. Chhiba, A. Tabyaoui, O. Mjihil, International Conference on Information Technology and Communication Systems (Springer, 2018).

[15] A. Lasbahani, M. Chhiba, A. Tabyaoui, O. Mjihil, A New Extension of Larman's Operation Contracts for Security Properties Injection and Verification during the System's Internal Behavior Elaboration, Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems, Vol. 33, pp. 1-6, November, 2017.