Applying Correlation and Regression Analysis to Detect Security Incidents in the Internet of Things

Daria Lavrova[1] and Alexander Pechenkin[2]

[1]Peter the Great Saint-Petersburg Polytechnic University, Russian Federation
[2]Peter the Great Saint-Petersburg Polytechnic University, Russian Federation,
lavrova.daria@gmail.com, alexander.pechenkin@ibks.ftk.spbstu.ru

***Abstract*:** In this paper, authors propose a complex of correlation-based methods for security incidents detection and investigation in large-scale networks of heterogeneous devices such as Internet of Things. Proposed methods aim to detect both known and unknown attacks in the Internet of Things.

***Keywords*:** Internet of Things, event correlation, security incident, regression analysis, correlation analysis, rule-based correlation.

1. Introduction

The Internet of Things (IoT) have been a current trend in information security, and the development of the IoT and its introduction in all spheres of human activity caused a large number of new security threats [1].

In accordance with [2], unknown attacks have a leading position among other for last 6 months (since December 2014 until June 2015). The complexity of security incidents detection in the IoT is based on a high heterogeneity of the IoT and on a low capacity of many smart devices, which does not allow integration with third-party protection means.

To overcome these problems one need to analyze huge amounts of heterogeneous data from the IoT devices. We propose a complex of methods, which is partly, solves a problem of security incidents detection in the IoT.

Proposed approach is inspired by an approach which is often used in security information and event analysis and management, such systems are called SIEM (security information and event management) [3]. SIEM systems primarily work with security events generated by various network security tools (such as firewalls, IDS, IPS etc), and the decision about security incident existence or absence is taken in accordance with the results of event correlation. Event correlation allows detecting interconnections between events from different devices. There are many different ways for event correlation such as rule-based correlation, statistical-based correlation, model-based correlation etc [4, 5]. For providing cyber security in the IoT, it is necessary to have methods for:

- Both known and unknown attacks detection
- Security incidents investigation

Proposed complex of methods aims to detect and to investigate security incidents and using this methods for detection both known and unknown attacks is possible.

2. Related Work

Proposed SIEM-based approach is also inspired by the work [6]. In this paper, authors propose an event-based concept for an autonomous adaptive risk management solution for the Internet of Things. Authors also propose to use event correlation for monitoring and detecting threats. In this paper authors describe several ways for event correlation, such as rule-base correlation, state machine automata based correlation, the codebook/correlation matrix techniques, anomaly-based approach, statistical correlation and probabilistic modeling. Authors primarily use rule-base correlation. The main difference and the novelty of our approach lies in implementation also a method for finding implicit and hidden relationships between events using correlation and regression analysis. This allows detecting new functional relationships between devices in the Internet of Things, which may display relationships which should not be. Such “bad” relationships characterize security incidents in the Internet of Things. So this approach allows to detect not only known attacks but also unknown attacks because such relationships may be caused by zero-day vulnerabilities, security leakages etc.

Also in our approach, as compared with the work [6], event correlation is investigated more deeply, by building event chains. That helps us to detect security incidents in the Internet of Things at an early stage.

Proposed complex of methods contains rule-base event correlation method that is a common approach used in a lot of research papers. In [7] authors propose correlation rules to define the relationship between physical and logical security events caused by abnormal behavior activities, that will helps to detect the multi-stage attacks. In [8] authors note that rule-based analysis is a classical approach to event correlation. That is, a correlation system constantly uses a set of predefined rules to evaluate incoming observations until a conclusion is reached. Therefore the correlation ability depends solely on the depth and capability of the rule set. Rule-based correlation method of detection priori insecure events proposed in our paper, works similarly, based on known attacks vectors in the Internet of Things and their manifestations.

In accordance with [9], anomaly detection is a common practice to ensure information security. In our work, we also use statistical-based correlation for monitoring anomalies in the Internet of Things events and their parameters. Statistical-based correlation does not employ any preexisting knowledge of the malicious activity, but instead relies upon the knowledge (and recognition) of normal activities, which has been accumulated over time. Ongoing events are then rated by a built-in algorithm and may be compared to the accumulated activity patterns, to distinguish normal from abnormal. In [10] authors proposed an approach which is based on a historical analysis of abnormality events with their probabilistic correlations. In [11] authors analyze the

use of different types of statistical tests for the correlation of anomaly detection alerts. Our statistical and rule-based correlation method of detection potential security events works similarly, but it also uses a rule-based approach for detecting security incidents.

Applying both correlation and regression analysis for providing cyber security in the Internet of Things is not widely covered. There are a sufficiently large number of works devoted to correlation analysis for providing information security in complex information systems including the Internet of Things. In [12] authors propose an assessment standard of how to calculating the threat factor and its weight value by analyzing the relationship between the utilization of the various factors, and decomposing the path on Internet of things system using the graph theory, probability theory and the correlation function.

Applying regression analysis methods for the IoT analytics is represented in works [13-15]. In [13] a multiple regression analysis is proposed to test whether the evaluations of the smart fridge after the scenario are related to their counterparts after interaction. In [14] authors propose a novel logit regression-based trust model called LogitTrust to model dynamic trust for service-oriented mobile ad hoc networks (MANETs) wherein a node can be a service requester or a service provider. MANETs are part of the Internet of Things implementation. In [15] regression analysis is applied to estimate the relationships between trust and a set of variables characterizing the behavior of a node.

The novelty of our method for finding implicit relationships of devices using correlation and regression analysis lies in applying a special coefficient that reflects the similarity in dynamics of two data sets. Data sets are represented as event parameters, collected for a certain period. Proposed method is based on an assumption that the series of interconnected data are changing similarly. Thus, interconnected events and interconnected devices could be obtained. When it becomes clear how devices are interconnected will be much easier to detect security incidents by regular monitoring of preserving or violation of relationships.

Proposed method for finding implicit relationships of devices using correlation and regression analysis is inspired by work [16]. In [16] authors proposed a security event correlation algorithm based on attribute similarity of mixed data type, which can refine the security event information and improve the availability of the security event information. This method is adopted to event characteristics of a proposed formal model of the Internet of Things event. For building event chains, we partly use an approach, proposed in [17]. This approach is based on event's clustering and correlation analysis between groups. In our approach, we add correlation analysis not only between security events but also between standard events for finding implicit correlations between clusters.

3. Features and Formal Models of IoT

Nowadays evolution of the IoT follows the trend of increasing intelligence of devices that are part of the IoT. This means that there is an increasing number of projects in which devices communicate with each other without human involvement. So the extent of human influence on the device functioning is minimized and eventually could be reduced to zero. Thus, the data for analysis is fully represents the data from the devices, each of which operates in accordance with a certain algorithm. For this reason, device's data analytics will give better results than data analysis from users whose behavior is difficult to predict.

Proposed complex of correlation-based methods consists of 4 methods:

- Rule-based correlation method of detection priori insecure events
- Both statistical and rule-based correlation method of detection potential security events
- Correlation and regression method of detection potential security events
- Event correlation method for investigation security incidents

Rule-based correlation method of detection priori insecure events aims to detect known attacks in the IoT. Statistical and rule-based correlation method aims to detect abnormal event characteristics by evaluation of statistical parameters, such as maximum, minimum, standard deviation etc. This method also uses rule-based correlation for detecting security events, but it is able to detect anomalies in data that could be an unknown attack's manifestation. Correlation and regression method of detection potential security events aims to find implicit interconnections in data from IoT devices and to reveal an analytical form of interconnections. Violations of these interconnections may indicate potential security incidents.

The last event correlation method for security incidents investigation aims to analyze interconnections between both security and standard events. On the basis of event correlation results event chaining building becomes possible, thus allows detect security incidents in the IoT at early stage.

For representation data from the IoT devices as an event there is one need to implement a formal model of an event, according to which large amounts of heterogeneous data from device will be aggregated and lead to a common sight due to the normalization. A formal model of an event is also needed for development the complex of security incidents detection methods.

Applied to the IoT an event represents in a form of tuple called event, describes the following information fields:

- Source
- Destination
- Action
- Date
- Time
- Functions

Event's parameter Source is a set of characteristics to uniquely identify the device that generates the event. $Source$ is described by IP address and ports of a device, and also by device ID. So, $Source = \{Source\_IP, Source\_id, Source\_ports\}$.

$Destination$ is a set of characteristics to uniquely identify the device that receives the event, $Destination = \{Destination\_IP, Destination\_id, Destination\_ports\}$.

$Action$ characterizes an event type, $Action = \{Message, Command, Unknown\}$. Date consists of three characteristics:

$Date = \{Date\_start, Date\_stop, Date\_abs\}$, where $Date\_start$ is a date from which event searching starts, $Date\_stop$ is a date until which event searching is performed, $Date\_abs$ is a date of logging an event in a system. Analogically, time characterizes time of event generation,
$Time = \{Time\_start, Time\_stop, Time\_abs, Time\_critical\}$. Here $Time\_start$ is a time from which event searching starts, $Time\_stop$ is a time until which event searching is performed, $Time\_abs$ is a time at which the event was logged in a system, $Time\_critical$ is a critical period.
There is also a set of functions for event processing:

- Get_Num
- Get_Value
- $Find\_Event$

Functions set: $Finctions = \{Get\_Num, Get\_Value, Find\_Event\}$.
Get_Num function determines the number of events, Get_Value determines the value of an event's characteristic, $Find\_Event$ function finds in logfile an event with appropriate characteristics. Thus an event is represented as a tuple:
$Event = \{Source, Destination, Action, Time, Functions\}$.

4. Rule-Based Correlation Method of Detection Priori Insecure Events

Under a priori insecure events to be understood events whose presence in the indicates a violation of the correct functioning of the IoT device / segment. Using rules-based correlation implies the description of a particular sequence of logical operations that characterize the actions of the attacker. With respect to the IoT, the use of rule-based correlation approach is offered subject to the availability of knowledge about how an attacker's action may affect the data from the IoT devices. To do this, it is advisable to study the existing classification of network attacks and attacks on the IoT. Knowledge from known attacks' classifications expands the list of developed rules and allows to improve an accuracy of detected attacks. Summarizing existing security incidents for the IoT, we reduce a priori insecure events to the following:

- Data absence from the device
- Connection with an IP-address from the black-list
- Error message
- Unknown type event

A data absence from the device can mean that the device is turned off or broken, that may characterize a potential security incident.
Rules are described using a formal language developed for submission to the correlation rules. This language combines the pseudo-code and mathematical and logical operators. Rules represent an algorithmic scheme, according to which developed rules are functioning, operators reflect the logic of finding the values of the parameters, or the number of investigated events described in accordance with the formal model of the event on the IoT. The main elements of a formal language are:

- Entities: event and the tuple's elements, $Event\_in\_List$, that means a set of events represented in a log file, $blackIPList$ etc
- Events' characteristics: $Values$ ($Value\_treshold$, $Value\_start, Value\_stop, Value\_current, Value\_error$ etc), $type$
- Mathematical operators: $=, \neq, +, -, <, >, \leq, \geq, \cup, \cap, \emptyset, \in, \cdot$
- Logical operators: $\rightarrow, \&, ||$
- Conditional operators: $if, for, then$
- Functions: $Get\_Num, Get\_Value, return$
- Alert signal: $alert!$

An address to a tuple's element is realized with the usage of square brackets, in which an event is written. For example, getting the type of event is written as $Action[Event]$.
An address to an element with certain type is realized with the usage of index. For example, if we want to sort only events with $Action = Message$, we use $Action\_type\ [Event] = Message$.
Indexing elements is also used to detail the object, assign it a label. For example, to mark a specific value from the device as erroneous, we use the error designation (error) as the index for the value: $Value\_error$.
The rule for detecting events indicating the absence of data on the device is as follows:

$for: Event\_in\_List$
{
$if\ (Source[Event] = Source\_current$
$\& Time\_abs[Event]$
$< Time\_abs[Event]$
$- Time\_threshold)$
$then\ n = n + 1$
}
$if\ (n = 0)$
$then\ alert!$

where:

- $Event\_in\_List$ – list of events
- $Source\_current$ – current value of event's source
- $Time\_abs[Event]$ – time at which the event was logged in a system
- $Time\_threshold$ – a threshold time value, in this case a response time
- n – is a variable counter
- $alert!$ – is an alert signal

Similar to this rule, the rest two rules are written. The rule for detecting events indicating an error message is as follows:

$for: Event\_in\_List$
{
$if\ (Action\_type[Event] = Message$
$\& Action\_value[Event] = Value\_error)$
$then\ alert!$
}

The rule for detecting events indicating a connection with IP address from blacklist is as follows:

$for: Event\_in\_List$
{
$if\ (Action\_type[Event] = Command$
$\& Source\_IP[Event] \in [blackIPList]$

$\& Destination\_IP[Event] \in [blackIPList])$
$then\ alert!$
}
Advantage of this rule-based correlation method is its high accuracy of security incidents detection. Disadvantages are need to regularly update the rules, inability to respond to situations that are not described in rules, therefore, inability to detect unknown attacks.

5. Both Statistical and Rule-based Correlation Method of Detection Potential Security Events

Potential security events could be caused by different event characteristics:

- Number of events, general or for a certain time period
- Values of the event tuple's elements

Potential security events caused by number of events are;

- Too many events from a device
- Too few events from a device

Potential security events caused by values of the event tuple's elements are:

- Element value is too big
- Element value is too little
- Element value significantly changes over time
- Violation of event's periodicity

First two types of events could be easily calculated. Special attention should be paid to an event, which characterizes significantly changes of an element value over time. The need to detect such type of events lies in a gradual increase of an attack intensity. Therefore, if event monitoring is carried out taking into account the recent changes, then calculation of new threshold values will include values, which are modified by an intruder. Due to this, the boundary values will gradually shift without an alert signal.
Calculation of threshold values is based on the standard deviation's calculation. Using a standard deviation, we can calculate an allowable threshold value for every event's characteristic. If the boundary is violated it will be an evidence of attack. Since in various times the load on a device can also be different, for the early detection of attack requires constant monitoring and counting of boundaries for each time step. This approach is inspired by works [18], in which authors analyze a problem of early DDoS attacks detection. In accordance with the results of experiments described in [18] the most perspective analysis method is the method which considering the seasonality. Detailed study of different kind of DDoS attacks and existing defense strategies is also represented in [19].
Let $x_i = Get\_Num\ (Event\_in\_List)$, where $Event\_in\_List$ contains events from the device for the certain period. Denote the number of daily periods as n. Then we can write all events from the device as a matrix:

$$\begin{matrix} x_{1\,1}\ x_{1\,2}\ x_{1\,3} \dots x_{1\,24} \\ x_{2\,1}\ x_{2\,2}\ x_{2\,3} \dots x_{2\,24} \\ \dots\ \dots\ \dots\ \dots\ \dots \\ x_{n\,1}\ x_{n\,2}\ x_{n\,3} \dots x_{n\,24} \end{matrix}$$

Each matrix row includes daily data about number of events. The first row represents the data of a current day, in this regard, it can be not completed until the end. The calculation is made on the columns of the matrix: $x_{n\,1},\ \dots,\ x_{2\,1},\ x_{1\,1}$.
If the device is using in accordance with weekly or diurnal cycle, it is necessary to exclude lines that match the festive and weekends.
Rules for detecting events which threshold values are calculated using this statistical-based approach are also described by correlation rules in the same formal language.
Advantage of this statistical and rule-based correlation method is its ability to detect anomalies in data and, consequently, to detect security incidents in the IoT in early stages. The main difficulty of this approach lies in a nicety of the right choice of periods, similar to each other.

6. Correlation and Regression Method of Detection Potential Security Events

6.1 Correlation analysis

Both previously presented methods are aimed at detection of security incidents, which manifested in the events from a single device. However, in case of providing security of the IoT it is necessary to use a "sensor fusion" principle. That means that the resulting information from combining of sensory data or data derived from disparate sources such has less uncertainty than would be possible when these sources were used individually.
Knowledge about interconnectedness of devices in the analyzed segment of the IoT will enable to detect unknown attacks because violations of interconnections may characterize a potential security incident. In addition, this knowledge helps in investigating security incidents.
Proposed correlation and regression method of detection potential security events includes two steps:

- Finding interconnections in data from the IoT devices
- Determination of an analytical form for identified interconnections

Proposed method is based on the assumption that in the analyzed segment of the IoT, where devices control each other without operator's influence (or with minimal influence), data sets generated by interconnected devices vary in concert and their dynamics is very similar. For this method uses correlation analysis for determination the existence of dependence, her strength and direction.
Linear interconnections could be found by using Pearson's correlation coefficient (or the correlation coefficient):

$$r = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \qquad (1)$$

where:

- X is a variable #1
- Y is a variable #2
- cov is the covariance
- σ_X is the standard deviation of X
- σ_Y is the standard deviation of Y

However, this factor can not reflect the existence of interconnection, if it is non-linear. For detecting non-linear interconnection, we use a special coefficient proposed in [20]. It is proposed to call the coefficient of similarity in dynamics. The degree of similarity in dynamics is investigated by estimation of the coefficients of the polynomial, which describes the initial set of observations, using the mathematical apparatus of finite differences. Formula of the coefficient of similarity in dynamics is as follows:

$$k_s = \frac{\sum_i \bar{\Delta}^i y \bar{\Delta}^i x}{\sqrt{\sum_i (\bar{\Delta}^i y)^2 \sum_i (\bar{\Delta}^i x)^2}} \quad (2)$$

where:

- x is a set of values of an estimated event's element for device #1
- y is a set of values of an estimated event's element for device #1
- $\bar{\Delta}^i x$ is a i^{th} order difference for x
- $\bar{\Delta}^i y$ is a i^{th} order difference for y

Derivation of the coefficient's formula is represented in detail in work [20].

In our research, we conducted an experiment. We took a dataset that characterizes the intensity of the automated blast furnace; it represents a nonlinear dependence between the hot blast temperature and the output per a single production mechanism. This dependence is not linear, because the rise of temperature can increase output only up to certain limits, beyond a some threshold intensity of output decreases.

Table 1. The normalized initial data

#	Hot blast temperature denoted as x	Output denoted as y
1	1,01	8,80
2	1,15	9,20
3	1,91	8,70
4	2,47	10,20
5	2,66	9,30
6	2,74	9,40
7	2,93	10,70
8	4,04	8,50
9	4,50	8,90
10	4,64	8,00

Analyzing the dynamics of the data series in accordance with a Figure 1, it can be concluded that the connection is not obvious.

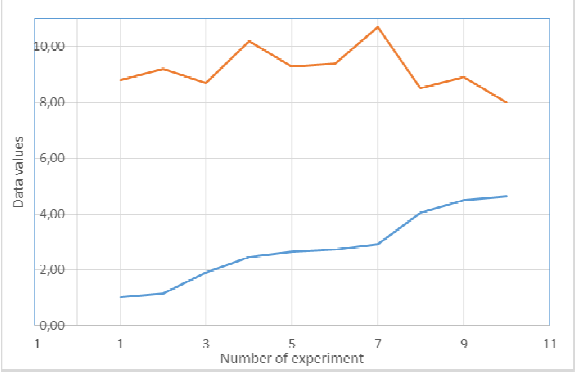

Figure 1. The dynamics of the data series

The calculated value of the correlation coefficient is -0,21, which leads to the conclusion that, at first glance, there is no interconnection between the two datasets.

However, the calculated value of the coefficient of similarity in dynamics is -0,63, that indicates a rather strong interconnection between these datasets. It is necessary to consider that this sample has a small volume, with increasing volume of data, value of the coefficient of similarity in dynamics will also be growing.

Thus, as a result of an experiment using machine data was revealed that the coefficient of similarity in dynamics is actually able to detect an implicit interconnection between two datasets. Consequently, it can be applied to identify interconnections in the IoT.

6.2 Regression analysis

The need to calculate the correlation coefficient in addition to the coefficient of similarity in dynamics is based on the fact that the proximity of coefficient of similarity in dynamics to 1 may indicate the existence of a strong nonlinear interconnection, while the value of correlation coefficient is close to 1 only in case of a strong linear relationship. Thus, the value of the correlation coefficient is a complementary factor for the second step of the method – an establishment of forms of analytic relationship.

Determination of an analytical form for identified interconnections based on the following approaches:

- Linear regression
- Nonlinear regression
- Extrapolation

Assuming a linear interconnection, we write the line equation in normal form and find its coefficients using the method of least squares. In the absence of a pronounced linear interconnection, experimental data is represented a curve line in accordance with a set of nonlinear functions, which are standard when trying to identify an analytical form of interconnection. If identifying an analytical form of interconnection using described regression approaches is impossible then we propose to use extrapolation for prediction of a set of future values.

List of standard using functions when trying to identify an analytical form of interconnection is as follows:

- A linear function $y = ax + b$
- An exponential function $y = ab^x$
- A rational function of the form #1 $y = \frac{1}{ax+b}$
- A logarithmic function $y = alnx + b$
- A power function $y = ax^b$
- A hyperbolic function $y = a + \frac{b}{x}$
- A rational function of the form #2 $y = \frac{x}{ax+b}$

In accordance with instructions proposed in [21], a regression form of the equation is:

$$\tilde{y} = f(x) + \varepsilon \quad (3)$$

Carrying out the calculations specified in [21] we could identify an analytical form of nonlinear interconnection between event's characteristics and, as a consequence, between devices.

The scheme of a correlation and regression method of detection potential security events is represented by Figure 2.

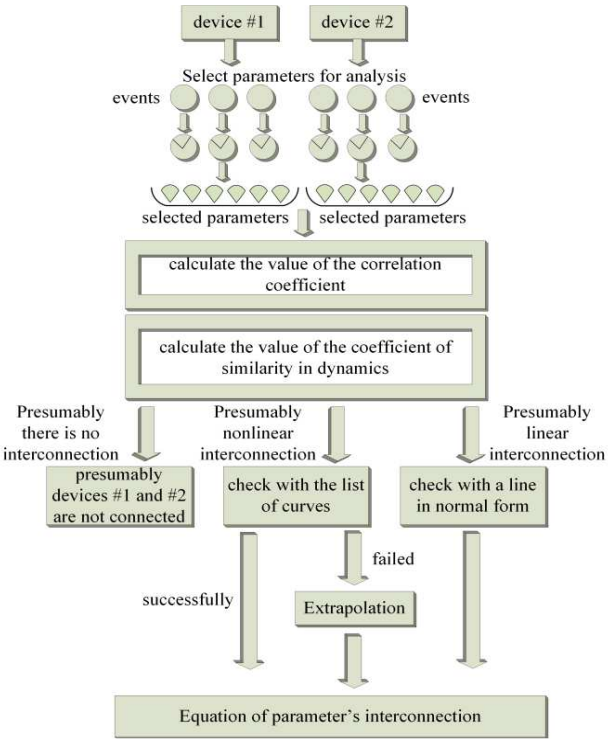

Figure 2. The scheme of a correlation and regression method of detection potential security events

7. Event Correlation Method for Investigation Security Incidents

After security incident was detected, it is necessary to investigate this incident to find vulnerable entry points in analyzed segment of the IoT. In this paper, we propose an event correlation method for investigation security incidents. Proposed method includes two steps:

- Correlation between two events
- Building an event-correlated chain

In the first step, we propose to correlate two events:

- Security event with security event,
- Standard event with security event,
- Standard event with standard event.

The second and the third correlation types are also advisable if an attack was skipped at an early stage so that an intruder penetrated in a protected segment of the IoT. In addition, there could be an insider in the protected segment and seemingly, legitimate actions may entail an attack characterized by security events.

Event correlation could be seen from calculation of similarities between them. In this method, similarity, and hence, correlation of events could be evaluated according to three parameters:

- Analysis of character parameters' correlation
- Analysis of numerical parameters' correlation
- Analysis of both character and numerical parameters' correlation

A general scheme for this method is described as follows.

- Depending on the type of security incident, which is supposed to detect, assign weight to each type of event's characteristics,
- Specify a correlation threshold, which would mean that if the correlation function takes a value greater than this threshold, then the events with sufficient force are correlated,
- Calculate the correlation between events using the correlation function,
- Compare an obtained value with a threshold correlation value,
- Group correlated events.

Further, it is advisable to calculate the correlation between the groups of events to build an event-correlated chain.

For calculation of the similarity between events, we use functions proposed in [22, 23].

The similarity function for character parameters:

$$Sim_{cha}(event_i, event_j) = \sum_{k=1}^{p} \frac{\varphi(value_{ik}, value_{jk})}{p}, \quad (4)$$

where:

- $\varphi(value_{ik}, value_{jk}) = \begin{cases} 0, (value_{ik} \neq value_{jk}) \\ 1, (value_{ik} = value_{jk}) \end{cases}$
- p is a number of character parameters of an event
- $value_{ik}$, $value_{jk}$ are values of character parameters of $event_i$ and $event_j$ respectively

The similarity function for numerical parameters:

$$Sim_{num}(event_i, event_j) = \frac{\sum_{f=1}^{n} \omega_f Sim_f(event_i, event_j)}{\sum_{f=1}^{n} \omega_f}, \quad (5)$$

where:

- ω_f is a weight of event's parameter designated as f;
- $Sim_f(event_i, event_j)$ is a similarity of parameter f between $event_i$ and $event_j$.

The similarity function for both character and numerical parameters:

$$Sim(event_i, event_j) = \mu Sim_{cha}(event_i, event_j) + 1 - \mu Simnum(eventi, eventj, \quad (6)$$

where μ is a weight coefficient that can be used to correct the numeric and character parameters in the contribution to the function of correlation between the events.

This method requires the development of efficient event clustering algorithms and their functioning in a high performance cluster. The complexity of development of this method could be in a reduction of accuracy caused by the incorrect assignment of weighting coefficients.

8. Conclusions

In this paper, we propose a complex of correlation-based methods for security incidents detection in the IoT. Providing cyber security in the IoT is a task, which topicality and complexity increases along with an evolution of the IoT. Proposed complex of methods aims to detect and to investigate security incidents and using this methods for detection both known and unknown attacks is possible.

The main contributions of this paper includes a novel approach for security incidents detection based on a finding implicit interconnections between data for different devices in the IoT. This approach is based on a calculation of the coefficient of similarity in dynamics. This coefficient indicates how similar are changes in time the values of two datasets. Such similarity may be caused by interconnection of these two data sets, and, consequently, may be caused by a functional interconnection between devices that generate analyzed data. We conducted a small experiment using the machine data of the blast furnace, and found that even a

small volume of a dataset is able to detect an interconnection.

Direction for our further works is to develop methods to collect and process data form the IoT in real time for rapid response to high critically security incidents.

9. Acknowledgement

Project is financially supported by Ministry of Education and Science of Russian Federation, Federal Program "Researching and Development in Priority Directions of Scientific and Technological Sphere in Russia within 2014-2020" (Contract No.14.575.21.0100; November 14, 2014).

References

[1] J. Shobana, B. Paramasivan, "GCCP - NS: Grid based Congestion Control protocol with N-Sinks in a Wireless Sensor Network," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 7, No. 2, pp. 99-105, 2015.

[2] Hackmageddon official (2015), http://www.hackmageddon.com.

[3] D. Cappelli, A. Moore, and R. Trzeciak, "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)," Addison-Wesley Professional, Cloth, 432 pp, 2012.

[4] Qishi Wu, Yi Gu, Xiaohui Cui, Moka, P., Yunyue Lin, "A Graph Similarity-Based Approach to Security Event Analysis Using Correlation Techniques," Global Telecommunications Conference (GLOBECOM 2010), Miami, Florida, USA, pp.1-5, 2010.

[5] P. Kabiri, A. A. Ghorbani, "A rule-based temporal Alert Correlation System", International Journal of Network Security, Vol. 5, No. 1, pp. 66–72, 2007.

[6] W. Aman, E. Snekkenes, "Event Driven Adaptive Security in Internet of Things," UBICOMM 2014 : The Eighth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Rome, Italy, pp. 7-15, 2014.

[7] D. Kang, J. Na, "A rule based event correlation approach for physical and logical security convergence," International Journal of Computer Science and Network Security, Vol. 12, No.1, pp. 28-31, 2012.

[8] G. Jiang and G. Cybenko, "Temporal and Spatial Distributed Event Correlation for Network Security", 2004 American Control Conference, Boston, June 30 - July 3, 2004.

[9] H. Jalali, A. Baraani, "Process Aware Host-based Intrusion Detection Model," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 4, No. 2, pp. 117-124, 2012.

[10] M. Marvasti, A. Poghsoyan, A. Harutyunyan, N. Grigoryan, "An Anomaly Event Correlation Engine: Identifying Root Causes, Bottlenecks, and Black Swans in IT Environments," VMware Technical Journal, Vol. 2, No. 1, pp.35-46, 2013.

[11] F. Maggi, S. Zanero, "On the use of different statistical tests for alert correlation: short paper", Proceedings of the 10th international conference on Recent advances in intrusion detection, Gold Goast, Australia, pp. 167-177, 2007.

[12] X. Jie, B. Hongjun, L. Yun, "Research on Security Threat Assessment Method Based on The Attack Tree Model of The Internet of Things," Journal of Convergence Information Technology, Vol. 8, pp.1-6, 2013.

[13] C. Floerkemeier, "The Internet of Things," IOT 2008, Zurich, Switzerland, pp.68-86, 2008.

[14] Y. Wang, Y.C. Lu, I.R. Chen, J.H. Cho, A. Swami, "A Logit Regression-based Trust Model for Mobile Ad Hoc Networks," 6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, pp. 1-10, 2014.

[15] J. Guo, I. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," 12th IEEE International Conference on Services Computing, New York, pp. 324-331, 2015.

[16] G. Zhaojun, Y. LI, "Research of Security Event Correlation based on Attribute Similarity," Research of Security Event Correlation based on Attribute Similarity, Korea, pp. 110-113, 2012.

[17] J.-H. Bellec, M-T. Kechadi, "Fuzzy Event Correlation Algorithm in Wide Telecommunication NetworksInternational Journal of Multimedia and Ubiquitous Engineering, Vol.3, No. 2, pp.103-116, 2008.

[18] O. Ternovoy, A. Shatokhin, "Reducing of error detection DDOS attacks using statistical methods, with considering the seasonality," Polzunovsky vestnik journal. Vol. 3/2, pp. 104-107, 2012.

[19] N.Ch.S. N. Iyengar, Arindam Banerjee, Gopinath Ganapathy, "A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 3, pp. 233-245, 2014.

[20] S. Svetunkov, I. Svetunkov, "Methods of socio-economic forecasting," Saint-Petersburg, Urait, p. 447, 2015.

[21] D. M. Patterson, R. A. Ashley, "Detecting Nonlinear Serial Dependence," Dynamic Modeling and Econometrics in Economics and Finance, Vol. 2, pp. 39-49, 2000.

[22] Z. Gu, Y. Li, "Research of security event correlation based on attribute similarity," International Journal of Digital Content Technology and Its Applications, Vol. 5, No. 6, pp. 222–228, 2011.

[23] J-H. Bellec, T-M. Kechadi, "Fuzzy Event Correlation Algorithm in Wide Telecommunication Networks," Journal IJMUE SERSC, Vol.3, no.2, pp.103-116, 2008.