View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by LSBU Research Open

Non-Conforming Behavior Detection for VoIP-Based Network Systems

Panagiotis Galiotos*, Christos Anagnostopoulos†, Tasos Dagiuklas*‡, Stavros Kotsopoulos*
*Dept. of Electrical and Computer Engineering, University of Patras
Patra, 26500, Greece
{pgaliot, kotsop}@upatras.gr
†Department of Digital Systems, University of Piraeus,Piraeus
Piraeus, 18534, Greece
chrisanag1985@gmail.com
‡Dept. of Computer Science, Hellenic Open University
Patra, 26335, Greece
dagiuklas@eap.gr

***Abstract*—This work proposes a detection scheme that identifies non-conforming behavior in a VoIP network, based on statistical analysis and hypothesis testing. VoIP networks are a popular, low-cost alternative for telephony that offer lower rates especially for long-distance calls. Other services such as FollowMe, enhance the traditional voice-oriented nature of these networks. Consequently several security concerns such as fraud calls, are related to the high availability required by a VoIP system. Fraud calls account for an average loss of 3% to 5% of the operators' revenue. Thus the detection and prevention of the users from behaving in a non-conforming way, becomes crucial. A trustworthy and secure management and billing scheme is necessary, to guarantee the proper operation. This work proposes a behavioral control scheme for the VoIP clients. An initial training period defines the normal behavior. Then statistical analysis and t-testing is employed to extract results regarding the users' profiles, with pre-defined confidence levels. A Buffer zone creates a more flexible decision-making process. The scheme also offers the ability to configure its parameters, in order to react appropriately under different network conditions and detect possible misuses. It is implemented and its rational operation is verified via several simulation scenarios.**

Keywords*—*VoIP fraud detection; Intrusion Detection System; T-testing; non-conforming behaviour; security

I. Introduction

The convergence of data and voice has been a fact for the telecommunication systems of the recent years. VoIP-based networks have gained widespread acceptance among the telecommunication systems. They offer a variety of services besides the simple voice calls, based mainly on the IP protocol. The most dominant protocol used nowadays is the Session Initiation Protocol (SIP). Platforms such as Asterisk are utilized to implement fully deployed VoIP-based solutions. However, this expansion of the VoIP systems has raised several security issues.

Service fraud is such an issue that costs an average percentage loss of 3%-5% of the operators' revenue [1]. This fraudulent behavior is realized through a series of attacks such as billing/dialplan configuration mistakes, usage of stolen credit card numbers, brute-force attacks to the Call Centers and hacking of the telephone or soft-phone devices. All these attacks usually results to (and can be identified by) alterations in the user's behavior. Hence misbehaving users must be detected and excluded from the provision of services in an effective and accurate way. This must be achieved in a non-disrupting manner for the rest of the system. It becomes obvious that the accuracy in the detection procedure and the small rate of false alarms are crucial facts for the smooth operation of the VoIP-based networks.

This work is based on a proposed detection scheme for wireless networks, that uses statistical analysis to extract decisions on the behaviour of certain nodes of the network [2]. The aforementioned detection scheme is enhanced appropriately to be adapted to VoIP service providers or systems, that operates based on contracts that predefine the behaviour and the rights of each user. The benefits of this work are twofold. First Intrusion Detection is utilized to introduce a scheme based on the Anomalous Behavior detection. In order to accurately define such a model, the Normal behavior of the system must be defined first, as precise as possible. This is done during the Training phase, where the system learns which behaviour is considered as normal for each user. Then the Detection scheme uses the extracted average values and applies them to the statistical analysis model, in order to calculate the deviation from this behavior and evaluate it, so that it can conclude whether this deviation is statistically significant and thus possibly caused by a fraudulent usage.

The second benefit of this work is that the system is implemented and tested, based on simulated Call Detail Records extracted from a fictitious VoIP operator, that represent certain normal, suspicious or malicious usage scenarios. Ideally these models should be produced, based on well-known distributions that represent all the main characteristics of a VoIP network such as Call Interarrival Times and Call Durations [3].

The remainder of this paper is organized as follows. Section 2 presents a wide range of previous work related to VoIP fraud detection and examines how it relates to ours. Section 3 describes the algorithm used for the detection, based on the pre-existing work and how this has been enhanced. Section 4 presents the implementation details and its operation. In Section 5 the simulation part of this work is presented, where

the implemented IDS scheme is tested using several fraudulent and normal VoIP-based scenarios. Finally, Section 6 concludes this paper by stating the main results and briefly mention the basic future directions.

II. Previous Work

Fraud Detection in Telecommunication Networks has gone a long way since the first research efforts to identify and systematically categorize the different types of frauds as well as the possible methods to recognize them. In the middle 90s, the authors in [4] propose a generic framework with some guidelines on how to categorize fraud activities and identify the most typical indicators of such behaviors. They suggest the anonymity of the data mining based on the Toll Tickets. Two main types of fraud detection are mentioned, namely the Absolute and the Differential Analysis. They discuss the advantages of Differential analysis such as flexibility and agility and how a User Profile is important for this procedure. Next they talk about the Rule-based approach and how fraud criteria are defined as rules. Finally they discuss the Neural network based approach which increases the intelligent of the detection system, something that is required for the highly heterogeneous fraud scenarios. The supervised and unsupervised learning methods are analyzed and the authors conclude that since none appears significantly superior to the other, both are investigated.

Attacks in VoIP Systems extend to a wide range. The authors in [1] mention both the vulnerabilities that are not specific to VoIP systems, such as denial of service, which can be handled by existing network security mechanisms, as well as threats related specifically to the nature of VoIP systems such as toll fraud, privacy and degradation of the quality of service, which can lead to a type of denial of service attack. The main reason is the clear text transmission of the packets from the VoIP protocols such as the H.323, the SIP and the RTP. They propose an IDS called SCIDIVE, with Cross-protocol detection, that involves packets from multiple protocols. Based on categorization of packets from different protocols, they create events, which when combined they lead to the formation of a more detailed rule that produces alarms with higher accuracy.

The authors in [5] describe several VoIP related threats that targets at either SIP or RTP protocols. They suggest that in order to more efficiently prevent these threats, the cross-protocol interactions needs to be examined, since VoIP comprises a plethora of protocols. Hence they propose a scheme that performs VoIP intrusion detection by utilizing the state machines of the protocols and the interactions among them to track deviations from interacting protocol state machines and provide intrusion detection with low runtime impact on the perceived quality.

In [6] a very informative analysis of VoIP fraud is presented. Firstly VoIP fraud is defined as the effort to avoid payment either by incorrect payment, or the lack of payment or the attempt to charge somebody else. The victims can be either the service providers or bigger enterprises such as AT&T. In particular, it is mentioned that in 2012, 46% of fraudulent calls were VoIP based. Then, the authors present a list with the most popular countries for originating and terminating fraud calls. The cost of a single VoIP fraud event ranges between 3K and 50K$ and the annual global losses between 30 and 50 billion $. These numbers definitely troubles the enterprises and the providers, since the losses range between 3 and 10 percent of their income. Finally it is worth mentioning that this type of fraud increases with a rate of 29% per year. The authors suggest that the best and simplest way to mitigate the results of these frauds is to analyze the Call Detail Record, in near real time and extract alerts or actions such as block a call. It is important to monitor the system during weekends, holidays and overnight where many of the VoIP frauds take place. Thus TransNexus implements a scheme that provides fraud detection by analyzing CDRs and observing possible, unusual traffic spikes that may lead to alarms or blocking actions.

The authors in [7] follow a different approach in securing VoIP systems, by proposing the use of Honeypots for intrusion detection in VoIP infrastructures. Actually they design a honeypot cloud, using several well-known honeypots in order to obtain valuable, realistic data from hacker VoIP attacks in the network and analyze them. They evaluate the performance of each honeypot and collect data such as malicious IP addresses. In the future such a honeypot data analysis can cooperate with an IPS for immediate reaction to security threats.

In [8], the authors propose a multilayer intrusion detection and prevention system for VoIP infrastructures. Specifically their work is based on the joint operation of a VoIP-specific honeypot and an application layer, event correlation engine. Any activity seen on the VoIP-specific honeypot is considered as a malicious one and the initiator as an attacker, since normally this system should not experience any traffic. At the same time, the event correlation engine is able to collect events from different sources in order to better realize the distributed nature of a VoIP system. These events are next fed as inputs to the event correlator, which acts as an anomaly based intrusion detection system. The goal is to achieve a holistic solution that can detect multiple types of attacks. Similarly to our work, the authors briefly mention the concept of anomaly-based intrusion detection with several specific metrics such as number of different recipients and number of calls, but no further analysis or implementation details are provided.

The authors in [9] propose a network-based intrusion detection mechanism, which uses a statistical Bayes model to detect intrusive SIP traffic. After examining the major VoIP-related threats, they present the weaknesses of some solutions such as the TLS and the S/MIME which heavily impact the performance. They proceed by modeling the SIP traffic in order to produce the Conditional Probability Tables, required by a Bayes model to detect several VoIP related threats such as SPIT, enumeration and DoS.

Hilas and Sahalos [10] presented a similar approach in several ways. Their main concentration is to construct certain profiles using PBX-based calls, that are used to determine whether a user is suspicious of becoming fraudulent. These profiles are based on eight features, that construct the user profile, such as the amount and the duration of Local calls, placed on a Telecommunication center of a Greek University. They extract the average values of these metrics and compare them with those of a later instant, trying to measure the similarity. The tool that they use for this purpose is the ANOVA test that performs k pair-by-pair t-tests. The main

differentiation of the present study is the introduction of the constant retraining and the Buffer zone, that brings a certain level of flexibility in the decision making. Hilas and Sahalos used the similar concept of equality interval, however the idea of monitoring based on a fuzzy decision is still missing.

Finally in [11] Rehabi et al. provide some interesting data on the state of VoIP fraud and its impact on the corresponding market. Specifically they claim that VoIP fraud accounts for a 3-5% losses of the annual revenue of operators and it is still increasing at a rate of more than 10% per year. Then they proceed by presenting the most known anti-fraud techniques which are divided into three main categories; the Rule-based techniques, the Supervised and the Unsupervised methods. The first category operates by using rules, which contain several conditions such as whether or not a suspicious transaction matches a blacklist. These rules can be combined with statistics. The second category refers to data mining and includes techniques such as neural networks, fuzzy logic and Bayesian networks. Then fraud patterns for both normal and fraudulent behaviors are constructed. The third category refers to the Unsupervised methods, where no prior knowledge about the observation classes in the dataset is required. In this case we do not know which transactions are legitimate and which are fraudulent. Hence profiles are created based on the cumulated past activity. The concept is that these profiles are used to predict the future behavior and any statistically significant deviation from that is considered suspicious and may conceal fraudulent activities. However, deeper investigation is required for these suspicious alarms. This method requires the mining of a huge number of CDRs. Our proposed Detection System (which will be described in the next section), belongs in the category of Unsupervised methods. The authors conclude their work by describing how the Scamstop projects tries to respond to the challenges of VoIP fraud by designing a Detection Framework.

III. Description of the Detection Algorithm

The proposed scheme for detecting fraudulent activity in VoIP networks can utilize features such as call duration or call inter-arrival time, that virtually describe a VoIP network in the call level. The analysis that follows is based on a statistical framework for abnormal behavior detection, proposed in [2]. That work was initially designed for wireless networks. It is altered to operate appropriately in a VoIP network with a multitude of heterogeneous users. Additionally, series of VoIP calls initiated by a specific user may be categorised as normal, malicious and suspicious, providing further flexibility in the detection phase.

Briefly, the proposed scheme performs Hypothesis testing, by using the t-testing method, in order to detect user behaviors that statistically deviates from what has been defined as normal, with a predefined significance level. The scheme can be deployed inside a VoIP system and examine the traffic produced by different users. Subsequently it attempts to determine if there is a significant possibility of fraudulent behavior. In such a case it posts an alert.

To successfully perform the detection, the False Negative (Type I) and the False Positive (Type II) errors need to be minimized. Therefore the scheme initially models the normal behavior of the system and quantifies it by extracting statistical properties, such as the mean and the standard deviation. This is called the Initial Training Phase of the algorithm. The accuracy and the overall performance of the fraud detection system also depends on the duration of the Initial Training Phase. The actual detection phase follows, by trying to compare recent traffic data with that of the training phase. If no malicious activity is detected, then the system performs a lightweight re-training to smoothly adapt to the dynamically changing behavior of the VoIP users. If a suspicious or malicious activity is detected, the re-training is suspended, until a final decision is made for this user.

After the detection phase, a user's behavior can be categorized as:

- *Normal*, where no threatening activity is detected.
- *Malicious*, where the behaviour significantly exceeds the user's normal activities and thus the system immediately characterize this user.
- *Suspicious*, where the current activity appears to deviates from its normal behavior. However, it is not obvious whether this is a possible malicious activity or simply a random event of increased traffic. In this case, the system considers this behaviour as suspicious, no decisions are made, the lightweight training process is suspended for that user (in order not to train the scheme in a possibly malicious behavior) and the system continues observing its activities to determine the actual status at a later stage, with higher probability of success. The user is considered to have entered the Buffer zone. If a user remains in the Buffer zone for a configurable number of consecutive time-periods, then the system identifies the behavior as malicious. Otherwise, the user exits the Buffer zone.

Decisions about the status of a user (malicious, normal or suspicious) are made throughout the time period of the operation. Note that the Buffer zone provides the scheme with some adaptability to possible behavioral changes. It can be appropriately configured, to adapt to the dynamic nature of a VoIP user and to absorb temporary bursts of its behavior. This is achieved by defining the values α and γ. The overall description of the system is shown in Figure 1:

The parameters that mainly quantify the VoIP user's behavior in the call level, are the following:

- *Call Duration*, for each registered user of the VoIP network.
- *Interarrival times of outgoing calls*, which describes the frequency that a registered user initiates calls.
- *Interarrival times towards a specific geographic location*, which describes the frequency of calls to a certain city.

By performing the Detection algorithm to these parameters, a wide range of attacks related to fraud calls, DoS to certain users/destinations or usage of stolen accounts can be eliminated. Currently the proposed scheme implements the Interarrival times of outgoing calls, by measuring the call rate of each user.

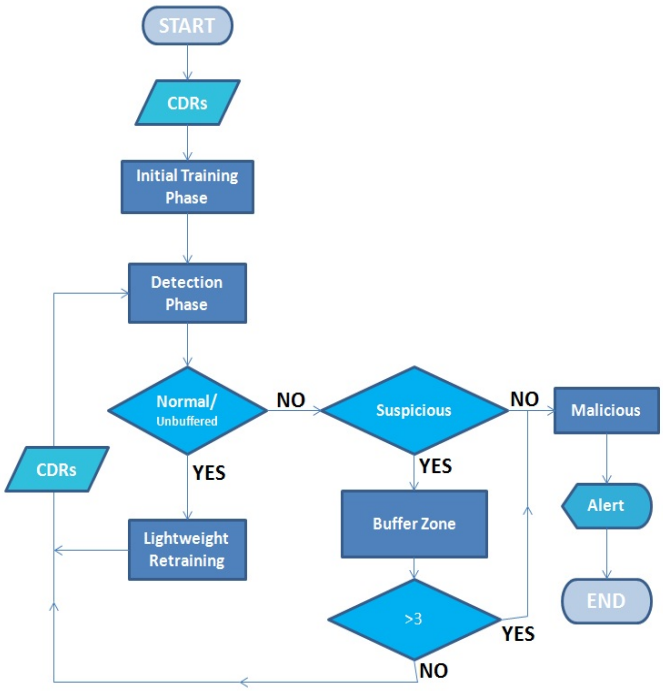

Fig. 1. Architecture of Detection Scheme

A. Initial Training Phase

The first part of the proposed scheme is the initial training phase. It is executed only once for each user and lasts for a pre-defined time period, called t_{tr}. During this time, behavioral features are extracted from the VoIP traffic, to construct the statistical model that describes the normal behavior. In particular this period is divided into a series of m sub-periods. The measured parameter is then calculated for each subperiod. The current version of the proposed scheme measures the *number of calls*, initiated by a specific user. This is denoted by $x_0(i)$, where 0 stands for the initial training period and i stands for the number of the sampling sub-period. Subsequently, the mean number of calls for the initial period is calculated and denoted by μ_0.

Similarly the standard deviation of the number of calls, is calculated by:

$$\sigma_0 = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}(x_0(i)-\mu_0)^2} \quad (1)$$

The total duration of the initial training period and the number of sampling sub-periods define the accuracy of the proposed scheme and can be decided by the network administrator, based on the characteristics of the VoIP system. The assumption made, is that the user's initial behavior is normal. An extended initial training period can lead to a more precise model, however this introduces the risk of accepting some fraud behaviors as normal. The number m of the sub-periods also affects the sensitivity of the model.

The initial normal behavior of each user is defined by the calculated mean and standard deviation. However, the scheme is retrained for each user throughout its lifetime, in parallel with the Detection Period. In that way, the algorithm can be re-trained to slightly changing behaviors of the user and increase the accuracy of the detection. This also makes the scheme more adaptable to the dynamic nature of the VoIP user over time.

B. Detection Phase

Next, the detection phase evaluates the statistical difference between the initial (normal) and the current behavior. It initiates after the initial training phase and continues throughout the system's operation, in parallel with the Re-training phase. It is partitioned in detection periods, each lasting t_{det} time. After each period is completed a decision is made, regarding the behavior of the active users during this time span. The algorithm continues to sample the number of successful calls. This number is denoted as $x_d(i)$, where $d1$ is the number of the detection period and i is the number of the sampling sub-period as stated above. For simplicity reasons it is assumed that $t_{det} = t_{tr}$ and the number of sampling sub-periods m remains the same. For each detection period the mean is denoted by μ_d.

The evaluation of the behavior alterations is based on the Hypothesis testing. The Null Hypothesis is defined as "The current usage is not fraudulent". This hypothesis is not rejected as long as the metrics of the current usage are statistically similar to those of the trained normal usage. The hypothesis is rejected if the metrics of two consecutive periods are found significantly different from each other. The significance level is decided by the significance parameter α. Thus, the scheme quantifies the False Positive (the error of rejecting the Null Hypothesis, while actually being true). Parameter γ is introduced to define the lower end of the Buffer Zone, which was earlier described. The selection of these parameters affect the Type I and Type II errors. The final decision is a tradeoff between retaining the credibility to the users and reducing the cost of these type of attacks.

The t-testing method is chosen to evaluate the Hypothesis:

$$t_d = \frac{\mu_d - \mu_0}{\sigma_0}\sqrt{m-1} \quad (2)$$

The proposed scheme applies the *one-sample t-test* to test the null hypothesis, since the normal behavior of a user is considered as the accepted value and its subsequent behavior is compared with that. Also, given that in the current implementation, lower mean values than the accepted ones are not of interest (since they express lower amount of traffic), the one-tail t-test is chosen.

Consequently, it is evaluated whether the difference between the current mean and the non-fraudulent mean of the training data is statistically significant. As shown in Figure 2, if a user is found in Zone 1, the Hypothesis is assumed to be true and the user is considered as Normal. Respectively, if found in Zone 3 this means that the difference is significant and the hypothesis must be rejected, hence the user is considered as possibly malicious. The confidence level of this decision equals to $(1-\alpha)$. The algorithm then generates an *Alert*. In case the behavior falls within Zone 2, then the user enters the

Buffer Zone and is further monitored. The p-value that follows the t-test, is utilized to identify in which Zone the statistical difference falls into.

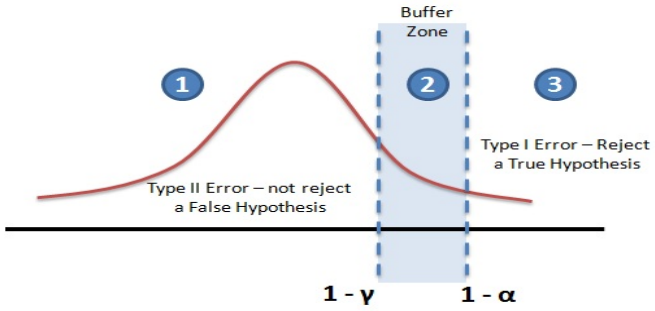

Fig. 2. The three Zones for evaluating the results of the one-tail t-test

C. Re-training Phase

As it was stated in the previous paragraph, the training continues throughout the lifetime of each user. In case the Detection phase concludes that the user's behaviour is normal, then the measurements of the current period should be incorporated in its behavior metrics. Subsequently the system needs to be re-trained based on this updated normal behaviour.

The proposed scheme employs the concept of the Exponential Moving Average, to implement the re-training of the system. Specifically, if the system is examining the n_{th} period of the user, then the updated expected behaviour $u\mu_n^i$ of user i is calculated by:

$$u\mu_n^i = (\mu_n) * \frac{1}{n} + (\mu_{n-1}) * \frac{n-1}{n} \quad (3)$$

Alternatively, if the user was indicated as suspicious before, and has already entered the Buffered Zone for one or more periods, the retraining of the system for this user has been suspended. If the user exits the Buffered zone in this current period, the system is required to be re-trained using not only the data of this current period but also of all the previous buffered ones. In general, the updated expected behaviour in case of exiting the buffer zone is calculated by:

$$u\mu_n^i = (\mu_n) * \frac{1}{n} + (\mu_{n-1}) * \frac{2}{n} + .. + (\mu_{n-k}) * \frac{n-k}{n} \quad (4)$$

where k is the number of possible buffering periods. The proposed scheme considers any user that remains buffered for more than 2 times as malicious, hence $k \leq 3$.

This type of re-training is as leightweight as required by a system that scales up to several thousands users, but also tries to appropriately capture the continually changing behaviour of the multitude of VoIP users, by avoiding a more static calculation.

IV. Implementation Analysis and Simulation Results

A. Implementation

The scheme is implemented as a proof of concept, in order to verify the rational operation of the proposed intrusion detection, under a multitude of different scenarios with simulated VoIP traffic. The implementation was realized using the Python programming language [12]. The pre-existing method *ttest_1samp* is employed, as it implements a two-sided t-test, using one sample of values that are statistically compared to the pre-calculated mean values that define the normal behavior.

The evaluated metric in the current version is the *call rate*, initiated by each user of the network. Part of the future work is to further develop other metrics, such as the *duration time* of the calls, in order to enhance the detection abilities of the scheme.

As stated before, the users are going through an initial training phase and subsequently the system is continuously retrained, to make the detection more precise in cases of minor alterations in the user's behavior.

Without loss of generality, if a user remains in the Buffer zone for three consecutive detection periods, it is considered as malicious. This number can be altered, depending on the period duration and the VoIP network's characteristics.

Finally, in case the system detects a user that continuously increases its call rate for more than five consecutive periods, it posts an alarm. Then the administrator/security engineer decides on the possible threat. Similarly, this number can be altered based on the network requirements and the level of sensitivity.

B. Results Analysis

Certain scenarios are designed, based on simulated CDRs, in order to verify the correct operation of the system. These scenarios simulate several normal and fraudulent cases, as well as some extreme cases in terms of user behavior. One such scenario simulates the case where the intrusion detection scheme smoothly adapts to a continuously changing behavior of a user, by going through the re-training phase. The examined scenarios are explained in more details, as follows:

1) *Scenario 1 - Normal user*, with a continuously changing behavior, which however does not significantly differentiates from its normal behavior.
2) *Scenario 2 - Buffered user that becomes normal again*, where certain random traffic spikes lead the system to characterize the user as suspicious and to observe it more carefully for some time period in the Buffer zone. At some later time and before being characterized as malicious, the user returns to its normal status and exits the Buffer zone.
3) *Scenario 3- Buffered user that becomes malicious*, where certain traffic spikes lead the system to characterize the user as suspicious (Buffer zone). After some observation time where its behavior continues to differ from the normal one, the system decides that the user is probably malicious.
4) *Scenario 4 - Malicious user*, where the user is detected directly as malicious, due to a significantly different behavior from its normal.
5) *Scenario 5 - Normal user with changing behavior*, where the user gradually but quite smoothly change its behavior and increases the call rate. The system is trained to this new behavior, without considering the

user as suspicious or malicious, due to the intensity of this change. However, the system issue alert signs when the user increases its call rate for several times in a row.

In general, the proposed scheme performed as expected in all five scenarios. Hence, a wide range of possible user behaviors are proven to be correctly identified by the proposed system. The results also showed that the accurate response of the scheme mainly depends on the configuration of the border parameters of the Buffer Zone. The α and γ values define the width of the Buffer Zone and consequently the possibility of detecting a user as Suspicious, Malicious or simply Normal. The presented scenarios produce different results when these limits are altered. For example, in one case a user is initially identified in the Buffer zone, and when the α and γ values are changed accordingly, then the same user is directly characterized as malicious.

In Scenario 2, an initially normal user is buffered for one time period, perhaps due to a random spike in its call rate. In the next period, the user returns to its normal behavior and the detection scheme unbuffers it and performs the retraining including the data of the previous period. Figure 3 shows the Current Mean of the user's call rate, as measured at the end of the detection period, compared to the Total Mean, measured up to the beginning of this current period. The p-value of the t-test performed for these two means in also presented, for this particular scenario.

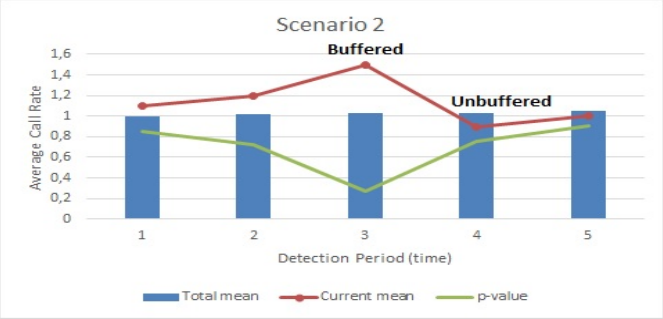

Fig. 3. A buffered user that is later unbuffered and becomes normal again.

Figure 4 presents Scenario 3, where a user, initially identified as normal, later enters the Buffer zone. The threshold for assuming that a previously buffered user is probably malicious, is set to three times. So the third consecutive time that a user is found in the Buffer zone, it is identified as malicious.

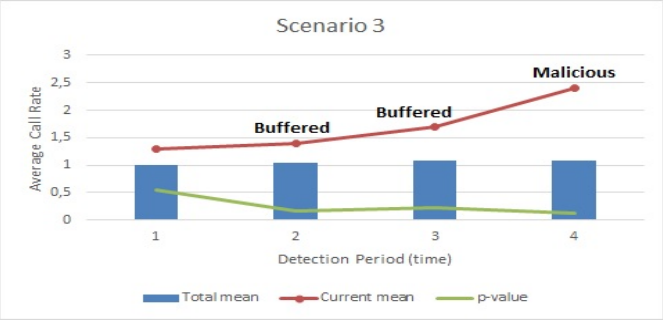

Fig. 4. A buffered user that is later identified as malicious.

Finally, Figure 5 shows Scenario 5, which refers to the case where a user gradually but steadily alters its initial behavior. In particular the user starts with an average of ten calls per period and concludes with twenty-eight calls per period. Despite the increase of 280%, the user is not detected as Malicious or even buffered during the scenario lifetime. This is due to its smooth and gradual change of the behavior, without any sudden increases or spikes in the produced traffic. Hence, the scheme proves to be able to learn the behavior of such a user and adapt. The downside of this feature, is that an educated attacker that can control its attack in an efficient way, can trick this scheme into accepting its behavior as normal.

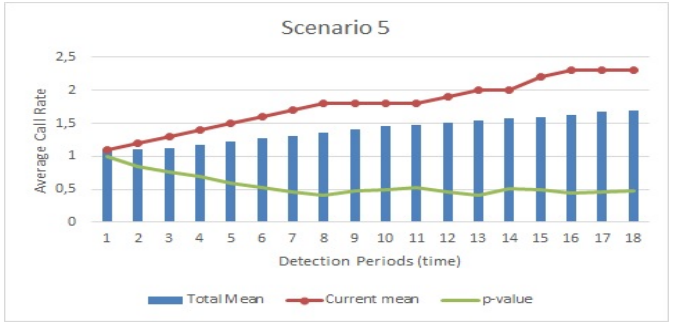

Fig. 5. The increase of the Call Rate is continuous but smooth enough, so that no malicious behavior is detected with the t-test and the p-value.

C. Sensitivity Analysis

As shown before, the one-tail t-test evaluates whether the Null Hypothesis should be rejected, by utilizing the Buffer zone. The Buffer zone is implemented by an upper and a lower level, which are defined by the values $1-\alpha$ and $1-\gamma$, as depicted in Figure 2. The sensitivity of the detection scheme mainly depends on these two parameters. By altering their values, the results may differ, even in the case of the same user executing the exact same scenario.

In particular, the value for the upper level $1-\alpha$, defines the difficulty of detecting a user directly as malicious. The value of the lower level $1-\gamma$, defines how easily a user is detected as normal. Lastly, the combination of these two values, defines the range of the Buffer zone and consequently the decision of characterizing a node as suspicious, which imposes to the system the overhead of continuously monitoring this user. If the the α and γ values are close, then the range is short and the probability of a user falling in the Buffer zone is small. This approach increases the decision speed of the scheme, however it can reduce its accuracy, since the decision is mainly based on unique events rather than on a longer monitoring. If the aforementioned values differ significantly, then a wide Buffer zone is created and the decision making procedure lasts longer but can be more accurate.

For example, Scenario 3 initially identifies the user as Buffered and then as Malicious. The α and γ parameters are set to 0.05 and 0.4 respectively. Next, the γ value is changed to 0.2, thus reducing the range of Buffer zone. The same scenario now considers the user as normal. Figure 6 shows the different output of the proposed scheme, for this user, during period 14, under the same scenario. Note that this is virtually equivalent to altering the significance level of the Hypothesis test.

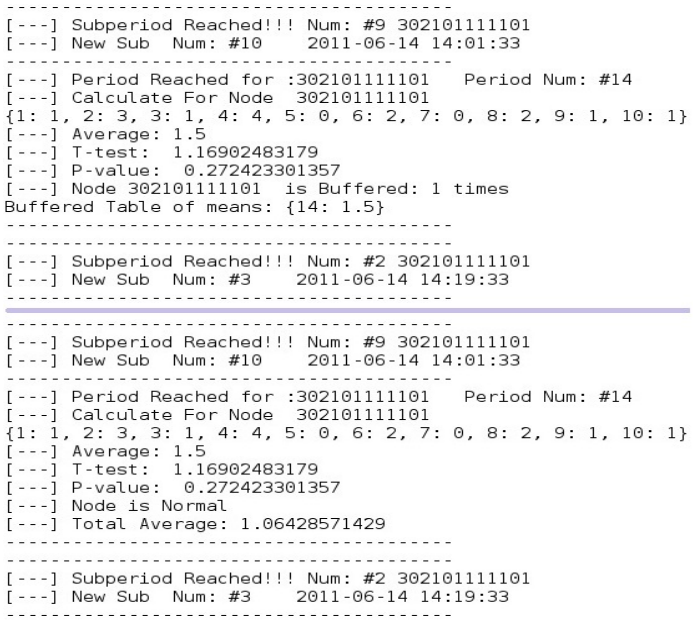

Fig. 6. The smaller buffer zone's range on the bottom, after decreasing the γ value, alters the decision of the proposed detection scheme

Note that in the case where the user is buffered (image on the top), no re-training is applied. Hence the Total Average remains unchanged, despite the case on the bottom image, where after the decision process, it is recalculated since the user is identified as normal.

V. Conclusion

This work presents a detection scheme for non-conforming behaviors in a VoIP network, using statistical analysis and more precisely hypothesis testing. The proposed design initiates with a training period, based on which the system is able to define the normal behavior for each user. The operational period follows, where the scheme calculates and compares the average values that characterize the user's behavior. Concurrently, a re-training period is performed for every normal user. In that way the security status of the VoIP system is continuously evaluated.

The scheme is implemented and tested under a variety of simulation scenarios, to verify the behavior of a VoIP-based system under specific requirements and conditions. All these scenarios were successfully completed and the expected results were obtained during the simulations. It is shown that the intrusion detection decisions are mainly dependent on the values assigned to the α and γ parameters and can adapt to changing behaviors. However, an educated attacker, under certain conditions, can train the system to identify its malicious behavior as a normal one.

The future work includes the performance of more realistic simulation scenarios, produced based on existing traffic modelling of VoIP data, in order to verify in a more precise way the operation of the proposed scheme. Comparison and evaluation with other detection schemes, in terms of credibility and performance, is also part of the future plans.

Acknowledgment

Part of this work has been performed in the framework of the project FP7-SME-2010-232458 SCAMSTOP, which is funded by the European Union.

References

[1] Yu-Sung Wu, Bagchi S., Garg S. and Singh N., *SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments*, Dependable Systems and Networks, 2004 International Conference on , vol., no., pp. 433- 442, 28 June-1 July 2004

[2] P. Galiotos, *Security-Aware Topology Control for Wireless Ad-Hoc Networks*, in the Proc of IEEE Globecom, New Orleans, USA, 30th Nov.-4th Dec. 2008.

[3] P. Galiotos, T. Dagiuklas, S. Kotsopoulos, *Call-level VoIP traffic modelling based on data from a real-life VoIP service provider*, to appear in IEEE Global Communications Conference, San Diego, CA, USA, 6-10 December 2015

[4] Yves Moreau, Peter Burge, John Shawe-taylor , Christof Stoermann, Siemens Ag , Chris Cooke Vodafone, *Novel Techniques for Fraud Detection in Mobile Telecommunication Networks*, 1996

[5] Sengar H., Wijesekera D., Haining Wang, and Jajodia S., *VoIP Intrusion Detection Through Interacting Protocol State Machines*, Dependable Systems and Networks, 2006. DSN 2006. International Conference on , vol., no., pp.393,402, 25-28 June 2006

[6] TransNexus, *Introduction to VoIP fraud*, White Paper, 2012.

[7] M. Voznak, J. Safarik and F. Rezac, *Threat Prevention and Intrusion Detection in VoIP Infrastructures*, International Journal of Mathematics and Computers in Simulation, Issue 1, Volume 7, 2013, ISSN 1998-0159, pp.69-76.

[8] M. Nassar, S. Niccolini, R. State and T. Ewald, *Holistic VoIP intrusion detection and prevention system*, IPTComm07 IPTComm07 Principles, Systems and Applications of IP Telecommunications, New York, NY, USA, July 19 - 20, 2007

[9] M. Nassar, R. State and O. Festor, *Intrusion detection mechanisms for VoIP applications*, Third annual VoIP security workshop - VSW'06 (2006), Berlin,Germany, June 1, 2006

[10] Constantinos S. Hilas, John N. Sahalos, *User profiling for fraud detection in telecommunication networks*, 5th International Conference on Technology and Automation, Thessaloniki, Greece, October 2005. pp 382-387

[11] Yacine Rebahi, Mohamed Nassar, Thomas Magedanz and Olivier Festor, *A survey on fraud and service misuse in voice over IP (VoIP) networks*, Information Security Technical Report, Elsevier, Volume 16, Issue 1, February 2011, Pages 1219.

[12] *Python Programming Language Official Website*, http://www.python.org/