Research Article

Toll Fraud Detection of VoIP Service Networks in Ubiquitous Computing Environments

Kyung-Il Kim,1 Taegu Kim,2 Nam-Wook Cho,3 and Minsoo Kim4

1Dial Communications, 133-2 Mokdongseou-ro, Yangcheon-Gu, Seoul, Republic of Korea
2Joint Chiefs of Staff, 22 Itaewon-ro, Yongsan-Gu, Seoul, Republic of Korea
3Department of Industrial & Information System Engineering, Seoul National University of Science & Technology, Gongneung 172, Nowon, Seoul 139-743, Republic of Korea
4Division of Systems Management & Engineering, Pukyong National University, Busan, Republic of Korea

Correspondence should be addressed to Nam-Wook Cho; nwcho@seoultech.ac.kr

Received 14 November 2014; Revised 6 January 2015; Accepted 13 January 2015

Academic Editor: Damien Sauveron

Copyright © 2015 Kyung-Il Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Voice over Internet Protocol (VoIP) is an emerging communication service that has advanced in ubiquitous computing environments. Although VoIP is inexpensive and offers additional services, there has been little provision for attacks at the weak points. With the advances of Wireless Sensor Network (WSN) technologies, the risk is increasing. Due to the resource constraints of WSN, attacks have become easier, making protection of the network more difficult. In this work, we attempt to distinguish fraud call attacks as outliers from normal calls on the basis of call detail records. We adopted and applied a Local Outlier Factor (LOF) method on real call data, which include actual fraud call attacks. Our results show the outlier detection method can be effective in detecting fraud calls. Moreover, introducing two additional attributes related to fraud call characteristics enhanced the detection performance.

1. Introduction

Voice over Internet Protocol (VoIP) is an emerging communication service that has advanced in both technological and industrial viewpoints. The prevalent usage of VoIP has led to increased attempts of toll fraud, which is defined as the unauthorized use of a telecommunications system by an unauthorized party [1]. Toll fraud often results in substantial additional charges for telecommunications services. Communications Fraud Control Association estimated global toll fraud losses in 2013 to be $46.3 billion (USD) [2].

The risk of attack is increasing in a ubiquitous computing environment with the emergence of Wireless Sensor Network (WSN) technologies. Recently outlier detection in WSNs has attracted much attention [3], as they are prone to outliers [4]. In particular, the resource constraints of WSN “make it easy to attach and hard to protect” [5].

Despite significant losses from attacks, there has been little provision for preventing attacks at the weak points on the networks. Existing fraud analysis applications rely on rule-based systems [6], in which fraud patterns are predefined by a set of multiple conditions. As a result, the fraud detection effectiveness is often limited. Relying on the knowledge of domain experts, a rule-based approach is ineffective in providing early warning; it is vulnerable to unknown and abnormal fraud patterns [7, 8]. In addition, as the threat of VoIP network increased in ubiquitous computing environments, preventing the VoIP fraud is critical to network service providers.

To overcome the limitations of existing approaches, we propose utilizing the Local Outlier Factor (LOF) method to detect toll fraud attacks. LOF is an outlier detection algorithm based on density in which call detail records (CDRs) from the VoIP service provider are used. CDRs document the details of
a phone call that passed through a facility or device. Recently, the LOF method has been successfully applied to outlier detection [9]. In [10], it is shown that LOF typically achieved better performance in network intrusion identification, compared with existing outlier detection algorithms.

Comparative experiments based on actual CDR from the VoIP companies have verified the effectiveness of the proposed approach. We expect that our proposed method will increase both efficiency and effectiveness of toll fraud detection in VoIP services, by overcoming the limitation of existing rule-based approaches.

The rest of this paper is organized as follows. In Section 2, relevant literature is reviewed and the LOF method is demonstrated. In Section 3, the structure of CDR data and experimental settings are included. In Section 4, experimental results are presented and their implications are discussed. In Section 5, we conclude our work and discuss directions of future work.

2. Background

2.1. Fraud Detection. Rule-based approaches and neural networks are examples of methods previously employed in toll fraud prevention. A rule-based approach uses predefined rules developed by experts. A notification is triggered when a rule is satisfied. As long as an effective set of rules can be defined, the rule-based method can be effective against fraud attacks. This method is ineffective for unknown types of fraud [7]. Rosset et al. [6] proposed a rule-discovery framework for fraud detection, in which candidate rules are identified first and the most relevant rules are selected on the basis of a suggested algorithm. Ruiz-Agundez et al. [11] proposed a rule-based fraud detection framework for VoIP services. In the proposed framework, a rule engine is generated using a knowledge base. Olszewski [12] attempted to construct user profiles on the basis of Kullback-Leibler divergence to prevent fraud detection.

Other fraud detection approaches include applications of neural networks, which can overcome the limitation of the rule-based approaches. While they can be more effective against unknown types of toll fraud, they also have limitations. Neural networks have difficulty presenting the interaction of cause and effect of detection. Burge and Shawe-Taylor [13] used a recurrent neural network technique based on unsupervised learning. Taniguchi et al. [14] proposed a feedforward neural network technique, a Gaussian mixture model, and a Bayesian network.

2.2. Local Outlier Factor. The LOF (Local Outlier Factor) is an outlier detection algorithm proposed by Breunig et al. [15]. The LOF has been applied in a variety of fields [16]. With the LOF, outlier instances are located distantly from neighbor instances in a multidimensional space, whereas normal instances gather relatively close to each other. Therefore, an instance with low proximity to its neighbor instances within a certain range can be regarded as an outlier. In this case, the relative index of isolation for the subject instance is defined as an LOF, which can be calculated by the following procedure.

\[
\text{reach-dist}_k(p, q) = d(q, p_k)
\]

(1) Calculation of k-Distance. For the subject instance \(q\), calculate the \(k\)-distance\((q)\) as the distance between \(q\) and its \(k\)th nearest neighbor.

\[
\text{reach-dist}_k(p, q) = \max \left( k\text{-distance}(q), d(p, q) \right)
\]

(2) Calculation of Reachability Distance. As depicted in Figure 1, the reachability distance is determined by the \(k\)-distance\((q)\). In detail, a reachable distance from an instance \(q\) to its neighbor instance \(p\) is defined as the maximum value of the simple distance between the instances. The \(k\)-distance\((q)\) can be written as follows:

\[
\text{reach-dist}(p, q) = \max \left( k\text{-distance}(q), d(p, q) \right)
\]

In other words, an \(\text{lr}\) is the reciprocal number of the average reachable distance to the neighbor instances.

\[
\text{lr}(q) = \frac{\text{MinPts}}{\sum_{p \in \text{MinPts’s nearest reach-dist}_\text{MinPts}} \text{lr}(p, q)}
\]

(3) Calculation of the Local Reachability Density. When \(\text{MinPts}\) indicates the number of neighbors considered, the local reachability density (\(\text{lr}\)) can be calculated using the following equation:

\[
\text{lr}(q) = \frac{\text{MinPts}}{\sum_{p \in \text{MinPts’s nearest reach-dist}_\text{MinPts}} \text{lr}(p, q)}
\]

\[
\text{LOF}(q) = \frac{1}{\text{MinPts}} \cdot \sum_{p \in \text{MinPts’s nearest lr}} \frac{\text{lr}(p)}{\text{lr}(q)}
\]

(4) Derivation of LOF. Finally, the LOF is derived by comparing the densities of the subject instance and its neighbors. This relative index is defined as the average ratio of the \(\text{lr}\) of a neighbor instance \(\text{lr}(p)\) over the \(\text{lr}\) of the subject \(\text{lr}(q)\):

Even though the LOF method is known to be effective in outlier detection, its application to CDR requires understanding and preprocessing of CDR data, which is explained in the next section.

3. Data and Experiment Setting

In our study, call detail records (CDRs) of a VoIP service were used. We collected two samples, including actual fraud call attacks. A specific product class of the target service provider
Table 1: Fundamental attributes.

| Attribute     | Description               | Note                                      |
|---------------|---------------------------|-------------------------------------------|
| Call time     | Start time of a call      | Unix timestamp                           |
| dst_length    | Length of destination extension | Excluding international call number   |
| Duration      | Duration of a call (after call time) | Seconds            |
| Billsec       | Duration of a call (after answering) | Seconds   |
| Disposition   | Code for call status      | 0 (answered), 1 (no answer), 2 (busy), and 3 (failed) |
| Uniqueid      | Instance’s ID             |                                           |

Figure 2: Call detail records data.

was selected, and then the CDR was obtained by routing those calls to an Asterisk server (http://www.asterisk.org). Figure 2 depicts a portion of the sample CDR data.

The aforementioned sample data consists of two separate datasets. Dataset #1 includes 105 fraud calls within 1,159 instances from June 29 to July 2, 2012. Dataset #2 includes 87 attacks within 2,062 calls from July 18 to July 20, 2012.

For each dataset, normalization was applied to resolve the differences in scale across attributes. Each column vector corresponding to an attribute was rescaled into the range \([-1, 1]\).

The original CDR data contained 18 unique attribute columns. In order to reduce complexity that might hamper the analysis and increase fraud detection effectiveness, we reduced the number of columns to six, as shown in Table 1.

In addition to the six primary columns, we introduced two additional variables for better detection, as shown in Table 2.

According to the settings on the attributes used, the experiment was conducted in two separate steps:

1. Experiment 1: analysis of datasets #1 and #2 using the six fundamental attributes;
2. Experiment 2: analysis of datasets #1 and #2 using the six fundamental and two additional attributes.

Tests were performed on MATLAB software with different MinPts: 10, 20, 30, and 40. Consequently, the top 2% to 10% of instances (with respect to the LOF values) were categorized into outliers. We assessed the performance by verifying whether the detected outliers successfully indicated actual threats.

In general, there are two criteria for the outlier detection performance. First, precision refers to the ratio of actual attacks among outliers or notifications that correctly identify the fraud call attacks:

\[
\text{precision} = \frac{n(FC \mid \text{outliers})}{n(\text{outliers})},
\]

where \(n(\text{outliers})\) denotes the number of outliers and \(n(FC \mid \text{outliers})\) indicates the number of actual attacks in the outliers. The second criterion is recall, which indicates the percentage of real attacks that can be prevented by the detection procedure:

\[
\text{recall} = \frac{n(FC \mid \text{outliers})}{n(FC)},
\]

where \(n(FC)\) is the total number of fraud calls in the test sample.

4. Results and Discussion

4.1. Experiment 1. In the first experiment, six attributes in Table 1 were utilized to produce LOF values. As seen in the performance measures shown in Figures 3 and 4, when the number of outliers increased from 2% to 10% of whole instances, higher recall and lower precision were obtained. We did not observe a conclusive trend with regard to the MinPts; we achieved the optimal performance when MinPts was set at 30 for both datasets.

With regard to outlier selection, we observed a significant difference between datasets. When a small set of outliers were selected (2–4% of total instances), the detection procedure exposed few actual threats for dataset #2, while the precisions were 10%–25% for dataset #1. However, for an 8%–10% outlier size, recalls on dataset #2 were quite higher than on dataset #1; some instances with the highest LOF values in dataset #2 were not actual fraud calls.

4.2. Experiment 2. In Experiment 2, we used two additional attributes: RTP address and country code to calculate the LOF values.

Figures 5 and 6 show a notable improvement in performance compared to the first experiment. Particularly for dataset #2, even with a small number of outliers, the precision and recall were quite satisfactory. Moreover, the intersubset difference was not as prevalent as in Experiment 1; the recall measures were found to be better on dataset #2 for Experiment 2. We also observed a correlation between the MinPts value and dataset performance. On both subsets,
Figure 3: Result for Experiment 1 on dataset #1.

Figure 4: Result for Experiment 1 on dataset #2.

Figure 5: Result for Experiment 2 on dataset #1.

Figure 6: Result for Experiment 2 on dataset #2.
Table 3: Comparison between Experiments 1 and 2 in terms of recall.

|              | Total | Data #1 | Data #2 |
|--------------|-------|---------|---------|
| Experiment 1 | 6.9%  | 9.9%    | 4.0%    |
| Experiment 2 | 32.5% | 27.8%   | 37.2%   |
| Significance at 1% | O     | O       | O       |

Table 4: Comparison between Experiments 1 and 2 in terms of precision.

|              | Total | Data #1 | Data #2 |
|--------------|-------|---------|---------|
| Experiment 1 | 9.2%  | 16.3%   | 2.0%    |
| Experiment 2 | 41.3% | 51.4%   | 31.1%   |
| Significance at 1% | O     | O       | O       |

a **MinPts** value of 10 resulted in poor precision and recall values.

To verify the difference between the results from both experiments, we executed a paired *t*-test on recall and precision measures. As summarized in Tables 3 and 4, two additional attributes induced improvements at 1% significance level, in terms of both recall and precision values on both subsets. The largest difference was found in dataset #2, in which recall improved by a factor of nine and precision improved by a factor of 15.

Overall, the experimental results have shown that the proposed approach can be effective for outlier detection of VoIP services, overcoming the limitation of existing rule-based approaches which are often ineffective for unknown types of fraud.

5. Conclusion

VoIP services have advanced both technologically and commercially with the emergence of broadband internet. However, due to the characteristics of the network it uses, the service is inherently vulnerable to various attacks. Additionally, detection and planning for these threats have not kept pace with advances in technology.

Our study proposed a detection method for fraud call attacks based on VoIP CDRs. The main idea of the suggested approach was that a fraud call exhibits a different CDR form; thus, it can be regarded as an outlier.

Among various techniques for outlier detection, we utilized the LOF method considering the difference in local density between the target instances and neighboring instances.

The LOF method produced limited results during the first empirical experiment on two sample datasets, which included actual fraud call attacks. However, these results improved considerably through the introduction of two additional attributes. Satisfactory performance in the second experiment demonstrated the LOF as an effective method to detect attacks, in addition to emphasizing the importance of selecting or designing meaningful attributes.

As our research on VoIP services was successful in fraud call detection, applying the LOF method on similar services would be an interesting research opportunity to investigate the differences according to the characteristics of target services. In particular, outlier detection in Wireless Sensor Networks (WSNs) is noteworthy, as WSNs are inherently prone to attacks and the LOF method can be easily applied to the outlier detection of WSNs.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the research program funded by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (MEST) (NRF-2013R1A1A2201169).

References

[1] Avaya, Avaya Toll Fraud Security Guide, Avaya, 2010.
[2] CFCA, Global Telecom Fraud Increases by 0.21% from 2011, Still Near 5-Year Low, Communications Fraud Control Association, Roseland, NJ, USA, 2013.
[3] Y. Zhang, N. Meratnia, and P. Havinga, “Outlier detection techniques for wireless sensor networks: a survey,” IEEE Communications Surveys & Tutorials, vol. 12, no. 2, pp. 159–170, 2010.
[4] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, “In-network outlier detection in wireless sensor networks,” Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, 2013.
[5] L. Huang, L. Li, and Q. Tan, “Behavior-based trust in wireless sensor network,” in Advanced Web and Network Technologies, and Applications, vol. 3842 of Lecture Notes in Computer Science, pp. 214–223, Springer, Berlin, Germany, 2006.
[6] S. Rosset, U. Murad, E. Neumann, Y. Idan, and G. Pinkas, “Discovery of fraud rules for telecommunications—challenges and solutions,” in Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 409–413, ACM, San Diego, Calif, USA, August 1999.
[7] S. Kim, N. W. Cho, Y. J. Lee et al., “Application of density-based outlier detection to database activity monitoring,” Information Systems Frontiers, vol. 15, no. 1, pp. 55–65, 2013.
[8] J. Yeon, J. Shim, and S. Lee, “Outlier detection techniques for biased opinion discovery,” The Journal of Society for e-Business Studies, vol. 18, no. 4, pp. 315–326, 2013.
[9] D. Pokrajac, A. Lazarevic, and L. J. Latecki, “Incremental local outlier detection for data streams,” in Proceedings of the 1st IEEE Symposium on Computational Intelligence and Data Mining (CIDM ‘07), pp. 504–515, IEEE Press, Honolulu, Hawaii, USA, April 2007.
[10] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, and J. Srivastava, “A comparative study of anomaly detection schemes in network intrusion detection,” in Proceedings of the 3rd SIAM International Conference on Data Mining, San Francisco, Calif, USA, 2003.
[11] I. Ruiz-Agundez, Y. K. Penya, and P. Garcia Bringas, “Fraud detection for voice over IP services on next-generation networks,” in Information Security Theory and Practices. Security
and Privacy of Pervasive Systems and Smart Devices, P. Samarati, M. Tunstall, J. Posegga, K. Markantonakis, and D. Sauveron, Eds., vol. 6033 of Lecture Notes in Computer Science, pp. 199–212, Springer, Berlin, Germany, 2010.

[12] D. Olszewski, “A probabilistic approach to fraud detection in telecommunications,” Knowledge-Based Systems, vol. 26, pp. 246–258, 2012.

[13] P. Burge and J. Shawe-Taylor, “Detecting cellular fraud using adaptive prototypes,” in Proceedings of the AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, pp. 9–13, 1997.

[14] M. Taniguchi, M. Haft, J. Hollmen, and V. Tresp, “Fraud detection in communication networks using neural and probabilistic methods,” in Proceedings of the 23rd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP ’98), vol. 1242, pp. 1241–1244, Seattle, Wash, USA, May 1998.

[15] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, “LOF: identifying density-based local outliers,” SIGMOD Record, vol. 29, no. 2, pp. 93–104, 2000.

[16] B.-Y. Kang, D.-S. Kim, and S.-H. Kang, “Extended KNN imputation based LOF prediction algorithm for real-time business process monitoring method,” The Journal of Society for e-Business Studies, vol. 15, pp. 303–317, 2010.
Submit your manuscripts at http://www.hindawi.com