Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 4, No. 4, November 2019, Pp. 337-344

Mitigating coordinated call attacks on VoIP networks using hidden markov model

Usman H. Nakorji *[1], E. A Adedokun [2], I. J. Umoh [3], Abdullazeez Shettima[4]
Ahmad Bello University, Nigeria[1,2,3,4]

Article Info
Keywords:
Coordinated Call Attack, VoIP, Short Term Energy, Hidden Markov Model, Call Interaction Pattern, Call Activities Detection

Article history:
Received 22 March 2019
Revised 25 June 2019
Accepted 31 July 2019
Published 30 October 2019

Cite:
Nakorji, U., Adedokun, E., Umoh, I., & Shettima, A. (2019). Mitigating Coordinated Call Attacks On VoIP Networks Using Hidden Markov Model. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(4). doi:http://dx.doi.org/10.22219/kinetik.v4i4.797

*Corresponding author.
Usman H. Narkoji
E-mail address:
harry14ng@gmail.com

Abstract

This paper presents a 2-tier scheme for mitigating coordinated call attacks on VoIP networks. Call interaction pattern was considered using talk and salient periods in a VoIP call conversation. At the first-tier, Short Term Energy algorithm was used for call interaction feature extraction and at the second-tier Hidden Markov Model was used for caller legitimacy recognition. Data of VoIP call conversations were collated and analyzed to extract distinctive features in VoIP call interaction pattern to ascertain the legitimacy of a caller against coordinated call attacker. The performance metrics that was used are; False Error Rate (FER), Specificity, Detection Accuracy and Throughput. Several experiments were conducted to see how effective the mitigating scheme is, as the scheme acts as a proxy server to Session Initiation Protocol (SIP) server. The experiments show that; when the VoIP server is under coordinated call attack without a mitigating scheme only 15.2% of legitimate VoIP users had access to the VoIP network and out of which about half of the legitimate users had their calls dropped before completion, while with the 2-tier mitigating scheme, when the VoIP server is under coordinated call attacks over 90.3% legitimate VoIP callers had their calls through to completion.

1. Introduction

Voice over Internet Protocol is a cost-effective and very efficient application for audio-visual communication businesses, this makes VoIP services prone to several attacks [1]. Telephony Denial of Service (TDoS) attack is a type of Denial of Service attack that target telephone services, like VoIP services, denying legitimate users access to the VoIP services [2]. These attacks are usually carried out during call transmission by disallowing honest users access to the VoIP service, example of aforesaid attacks are SIP flooding attack and VoIP amplification attack [3]. They are usually achieved by generating immense number of calls at an instance and direct the large traffic through its targeted VoIP server, these attack patterns can easily be detected by network administrators and by placing a good monitoring tool that analyses the network flow and whenever there is unusual increase in traffic it activated the mitigating tool to block IPs [4].

There is a current category of Distributed Denial of Service (DDoS) attack known as Application- Layer Distributed Denial of Service attack (ADDoS), this recent form of DDoS attacks can bypass the traditional mitigating systems that only monitors unusual increase in network traffic then block the IPs of the unusual traffics [5]. ADDoS is a kind of attack that is not actualized over the network layer, but across application layer [6]. This means that the ADDoS attacker can aim at a specific application of its target server, while other applications are running, thereby generating less traffic and making the attacker very difficult to detect [6]. This is possible because the attacker generates very similar traffic to that of a legitimate user [1]. Here are types of ADDoS attacks namely; POST attack, Slowread attack, Slowloris attack, attacks exploiting protocols used by HTTP and then Coordinated Call attack that target VoIP services [7].

This research focused on mitigating Coordinated Call attack. Coordinated Call attack is conducted when two attackers that are equally registered to VoIP system pair up and put a call to each other, through a targeted VoIP server and then stay on calling state and remains in the state for as long as possible thereby exhausting the victim’s VoIP server resources [8]. It is known that VoIP servers allocate resources to each call, therefore by using several pairs of call channels simultaneously, they can take down a target VoIP network by exhausting resources of the server since each VoIP server has a number concurrent calls it can take at a time [9].

Coordinated Call attack is relatively a new attack, there are not many studies on how to mitigate them, while there is abundance of traffic data for DDoS at Network layer targeting VoIP services to work with, such as; CAIDA databases, UNINA database and KDD Cup database, the case is different for Coordinated Call attack (ADDoS).

At call interaction features extraction stage, Short Term Energy (STE) was computed by breaking the signal of voice into frames of M samples and then computed the total squared values of the samples within each frame [10]. This breaking of the audio signal was attained by the use of a right window function to split the voice signal into required frames [11].

While at call interaction pattern recognition state, Hidden Markov Model (HMM) was trained with extracted features from STE module. This enables the HMM to drop coordinated call attackers calls as perceived. These HMMs contain transition distribution state, observation state and initial distribution state [12].

Diverse types of approach were used to mitigate DDoS attack aiming VoIP systems [13][14][15]. They built their mitigation system to analyze network traffic flow into the VoIP server and when a large and unusual traffic is detected, the system activates its defense mechanism. A selective strategy was developed to mitigate Coordinated Call attacks on VoIP servers. This mitigated the attack effectively, but it was clouded by huge number of drop calls. Hence, the contribution of this research is:

1. To develop a Short Term Energy (STE) Scheme for mitigating Coordinated Call Attacks on VoIP networks based on Hidden Markov Model (HMM) called STEHMM.
2. To simulate STEHMM used for classification of callers on VoIP server when under coordinated call attack using Java.
3. To design a scheme that works perfectly with VoIP SIP server
4. To select call parameters that will reduce number of drop calls to its barest minimum in the course of mitigating coordinated call attack on VoIP network.

2. Research Method

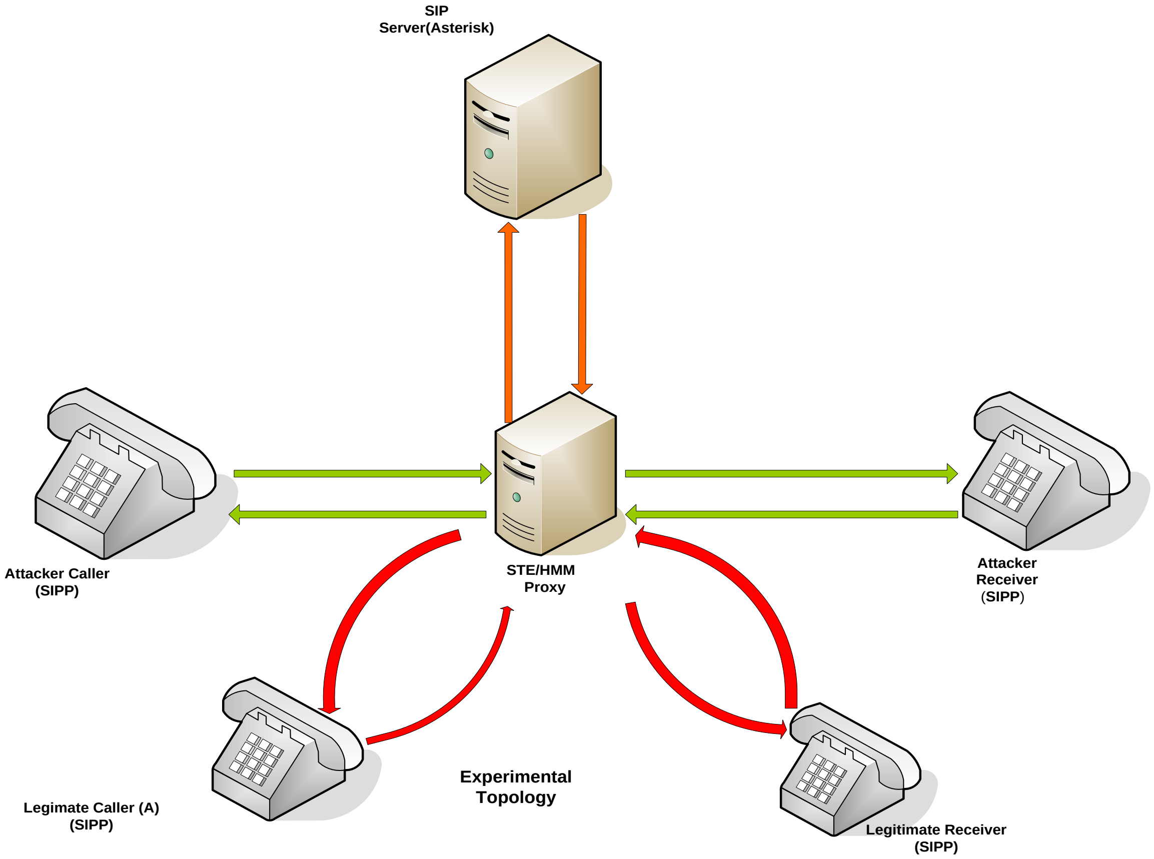


Figure 1. Experimental VoIP Network Architecture

Figure 1 above is the experimental VoIP network architecture used to mitigate coordinated call attack and to test the effectiveness of the developed STEHMM. When a VoIP call is put through Session Initiation Protocol (SIP) server through the STEHMM server as a proxy as shown in Figure 1 above, the STEHMM server consists of two tiers which are: call feature extraction tier which is handled by Short Term Energy (STE) algorithm and call feature pattern recognition tier which is handled by Hidden Markov Model (HMM). Data of VoIP call conversations were collated and analyzed to get distinctive features for legitimate caller, coordinated calls, attacker's calls and robot or pre-recorded calls see Figure 2.

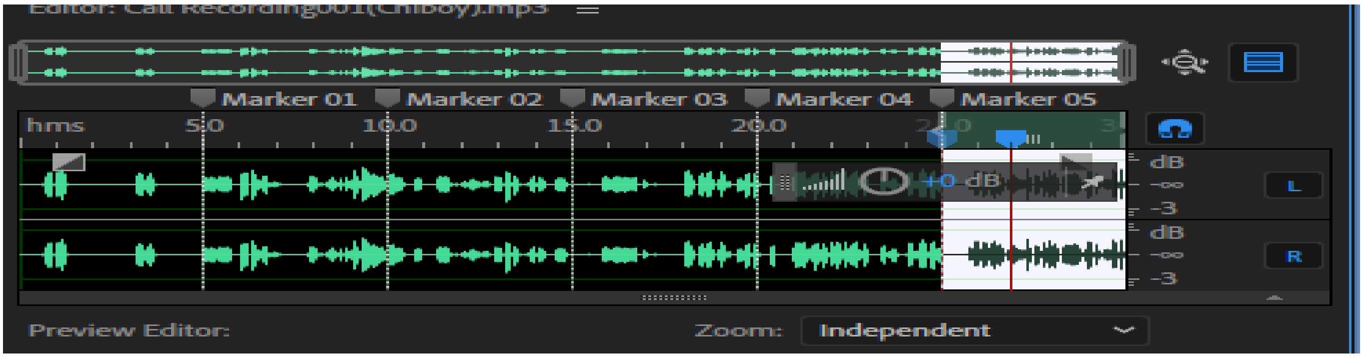


Figure 2. A Snippet of 30 Secs Legitimate Call Interaction Waveform

Table 1. Extracted Features and Parameter Weights For 30 secs Frame of 5secs Window Call Interaction

Windows	5secs	10secs	15secs	20secs	25secs	30secs
Weights	0.06, 0.05	0.15, 0.14	0.18	0.02	0.06	0.15
Call interaction features	s_6, s_1	s_2, s_5	s_3	s_4	s_6	s_2

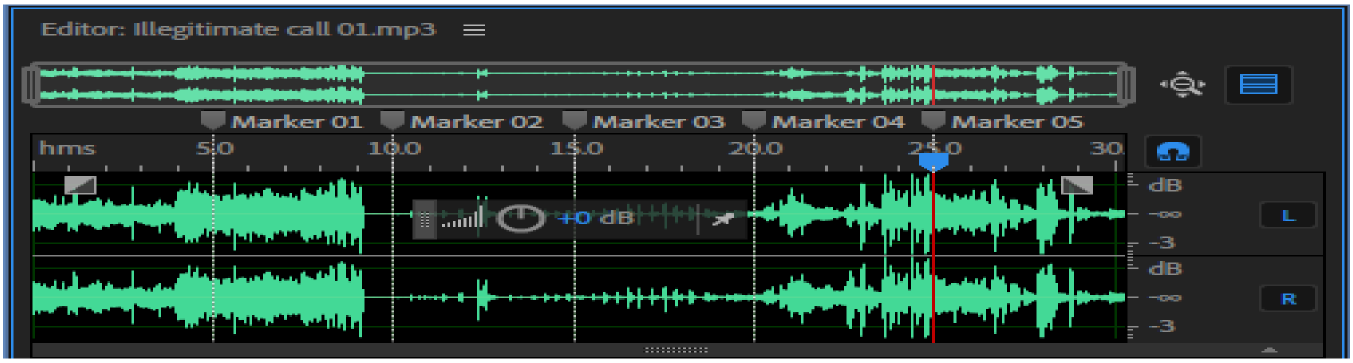


Figure 3. A Snippet of 30 Secs CCA Call Interaction Waveform

Table 2. Extracted Features and Parameter Weights for 30secs Frame of 5secs Window Call Interaction

Windows	5secs	10secs	15secs	20secs	25secs	30secs
Weights	0.05, 0.15	0.15, 0.18	0.02	0.15	0.05, 0.15	0.05, 0.15
Call interaction features	$s_1, s_2,$	$s_2, s_3,$	$s_4,$	$s_2,$	s_1, s_2	s_1, s_2

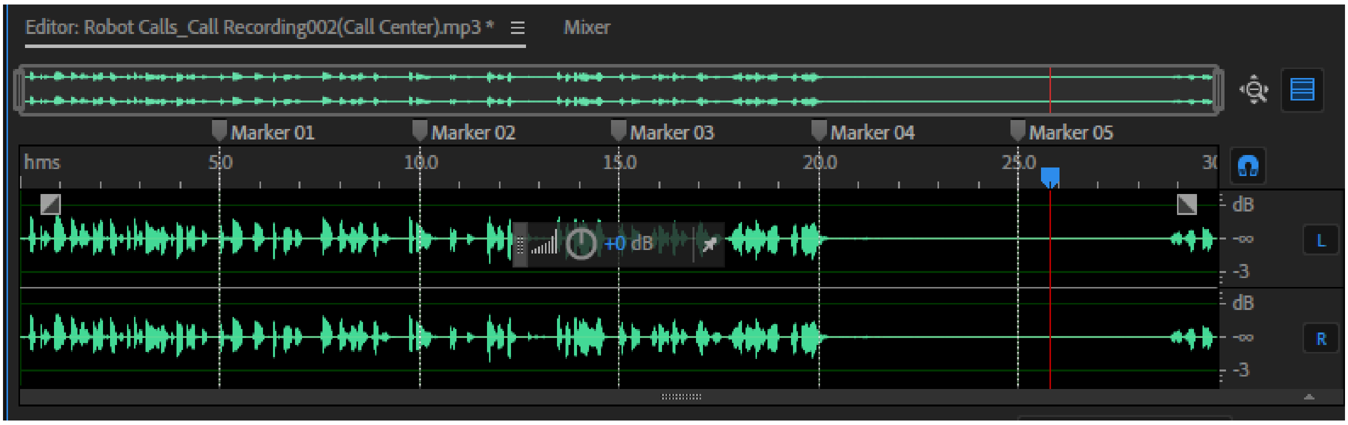


Figure 4. A Snippet 30secs Robot Call Interaction Waveform

Cite: Nakorji, U., Adedokun, E., Umoh, I., & Shettima, A. (2019). Mitigating Coordinated Call Attacks On VoIP Networks Using Hidden Markov Model. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(4). doi:http://dx.doi.org/10.22219/kinetik.v4i4.797

Table 3. Extracted Features and Parameter Weights for 30secs Frame of 5secs Window Call Interaction

Windows	5secs	10secs	15secs	20secs	25secs	30secs
Weights	0.05	0.05	0.05, 0.15	0.05	0.15	0.15
Call interaction features	s_1	s_1	$s_1, s_2,$	s_1	s_2	s_2

The above, Figure 2, Figure 3, Figure 4, and Table 1, Table 2, and Table 3 were repeated for attacker's call interaction pattern and for a pre-recorded VoIP call and the following features were extracted and their corresponding STE weights. Features from VoIP call conversation between party A and B was considered, the feature are; A talking and B is silent (AT/BS), A silent and B is talking (AS/BT), Mutual silence where A spoke last (MS/AL), Mutual silence where B spoke last (MS/BL), Double talk where A interrupted (DT/AI) and Double talk where B interrupted (DT/BI) which are represented as s_1 s_2 s_3 s_4 s_5 and s_6 respectively. The corresponding STE E_n for s_1 to s_6 were taken using the Equation 1.

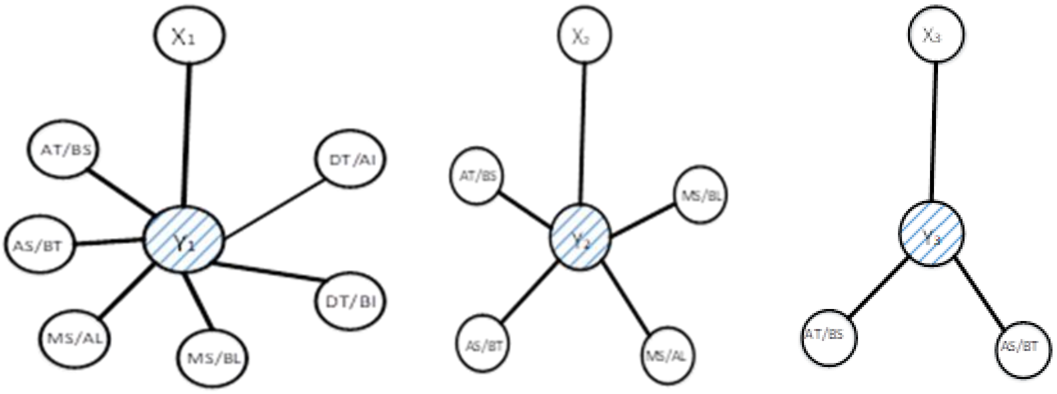
$$E_n = \sum_{m=-\infty}^{\infty} (x(m).w(n-m))^2 \qquad (1)$$

Where E_n represents the nth frame of Energy for the voice activity signal as $x(m)$ denotes amplitude for the voice activity signals in time domain and $w(n-m)$ is the window function where the samples are. The energy E_n of each identified call interaction pattern is calculated for every 5secs hamming window within each 30secs frame for each pattern $w(n-s_i)$ of VoIP call conversation [11]. The energy is calculated, such that, when a pattern is identified within a window it drops the calculation of that particular energy and calculates the next pattern to avoid loop of recalculating an already identified pattern the corresponding STE are tabulated on Table 4.

Table 4. STE Weight Values Assigned to Call Interaction Parameters

SN	Simulation Parameter	Weight (Joules)
1	s_1	0.05
2	s_2	0.15
3	s_3	0.18
4	s_4	0.02
5	s_5	0.14
6	s_6	0.06

The STE weights in Table 4 were further used to train three HMM models that were developed, of the three HMM models, one has combination of s_1 to s_6 representing legitimate caller, the second HMM has combination of s_1 to s_4 representing coordinated call attacker caller and the third HMM has combination of only s_1 and s_2 for robot caller, these are schematically represented on Figure 5.



(a) (b) (c)

Figure 5. HMM Model Call Interaction Pattern Recognition (a) HMM for Legitimate Caller (b) HMM for CCA Attack Caller (c) HMM for Pre-Recorded Caller

Asterisk 13.6.0 was used for call management, 50 callers maximum was set, When the VoIP server is saturated, that is, incoming calls are unable to complete the call initiation process and kept in WAITING or USER BUSY mode, which signifies the VoIP server has attained its 50 calls bound, the scenario where VoIP server is under CCA attack, out of the 50 calls it was observed that 60% of the calls ongoing are legitimate callers and 30% are illegitimate callers and 10% were robot callers, which was our initial prior in HMM $P(x_0) = \{0.6, 0.3, 0.1\}$. The table below contains the energy weights for the six talk interaction patterns deduced from VoIP call conversation, the weights are chosen from the STE waveforms of each talk interaction pattern. These patterns as extracted are represented as; s_1 s_2 s_3 s_4 s_5 and s_6, with weights attached to patterns in joules as obtained from the collated VoIP call conversations which are then compared to the observation state of HMM model $B\{y_{1,} y_{2,} y_3\}$ to determine the hidden states x_1, x_2, x_3. The HMM parameters as defined for caller identity below

Where HMM is Equation 2.

$$\lambda i = (Ai, Bi, \pi i) \tag{2}$$

And;

$\pi =$

x_1	x_2	x_3
0.6	0.3	0.1

the above π is the initial distribution state.

$P(X_t|X_{t-1}) =$

$P(x\|y)$	y_1	y_2	y_3	y_4	y_5	y_6
x_1	0.3	0.2	0.1	0.1	0.2	0.1
x_2	0.4	0.3	0.2	0.1	0	0
x_3	0.6	0.4	0	0	0	0

1 ≤ i, j ≤ 6

The table above is the transition distribution state A.

$Bi =$

$P(x\|y)$	y_1	y_2	y_3	y_4	y_5	y_6
x_1	0.1	0.3	0.1	0.3	0.1	0.1
x_2	0.1	0.4	0.2	0.3	0	0
x_3	0.5	0.5	0	0	0	0

Finally, B is the observation state distribution that allow transition amongst states. The tucker conditions for the HMM models λ dropping attacker's call as perceived is given as.

$$f(\lambda) = \begin{cases} x_1, & if\ 0.5 \geq y_1 \leq 0.6 \\ x_2, & if\ 0.2 \geq y_2 \leq 0.3 \\ x_3, & if\ 0.05 \geq y_3 \leq 0.1 \end{cases}$$

3. Results and Discussion

This paper used asterisk server which is predominantly used for small and medium scale businesses. The maximum concurrent calls were set to 50 callers, the 50 calls were varied at ratios; 10:40 calls, 20:30 calls, 30:20 calls and 40:10 calls of coordinated call attackers to honest VoIP users to observe the effect of the attack at each ratio. Three experiments were conducted, the initial experiment was conducted with VoIP server under coordinated call attack without using any mitigation scheme, the second experiment carried out was when the VoIP server is under coordinated call attack and using STEHMM to mitigate it and lastly, when the VoIP server is not under coordinated attack with STEHMM.

The experiment conducted when the VoIP server was under coordinated call attack without using STEHMM to mitigate shows that only 15.2% of VoIP users were able to make call through the VoIP server. 30.1% of the those who had their calls through got their calls terminated before call completion.

The second experiment conducted when the VoIP server is under Coordinated call attacks and using STEHMM for mitigation shows STEHMM mitigated coordinated call attack effectively. This is due to the fact that 90.3% VoIP callers had access to the VoIP server. However, out of the 90.3% about 8.2% users had their calls terminated before they could complete their calls.

The last experiment was carried out to see the burden STEHMM has on the already overburdened VoIP network. STEHMM has no negative effect on the VoIP network, this is because as soon as coordinated call attack is mitigated STEHMM goes to passive mode to save the network resources.

The bar chart in the figure below shows the experimental results of the first sets of experiment conducted to see the effect of coordinated call attack on VoIP networks before applying a mitigation scheme.

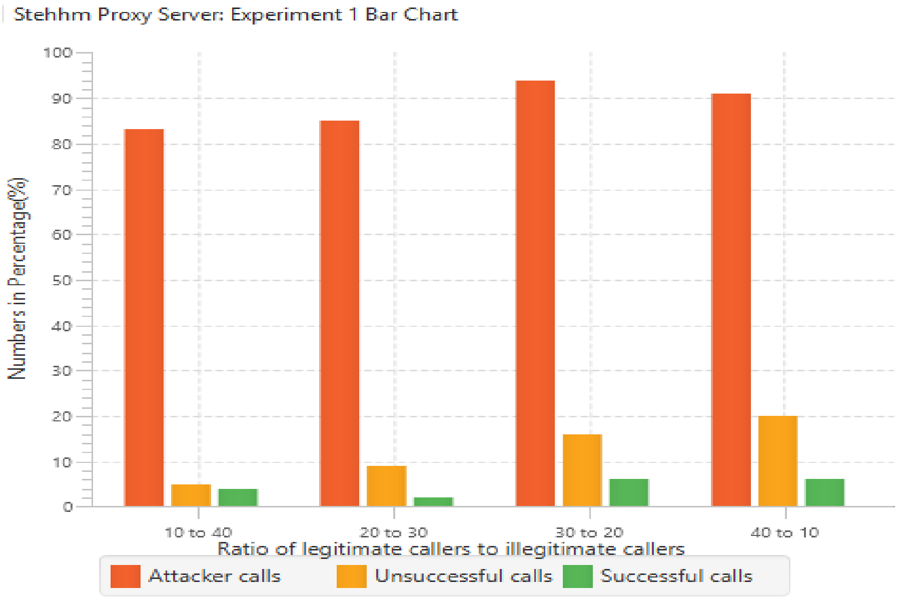


Figure 6. VoIP User Success Rate When Under CCA Without Mitigation

The bar chart in the Figure 6 above shows that, when a VoIP server is under coordinated call attack without using a mitigation scheme only 15.2% of the legitimate VoIP users had access to VoIP server while 30.1% of them had their calls terminated before completion.

The bar chart in the Figure 7 below shows the experimental results of the second sets of experiment conducted to see the effect of STEHMM on VoIP networks when under coordinated call attack.

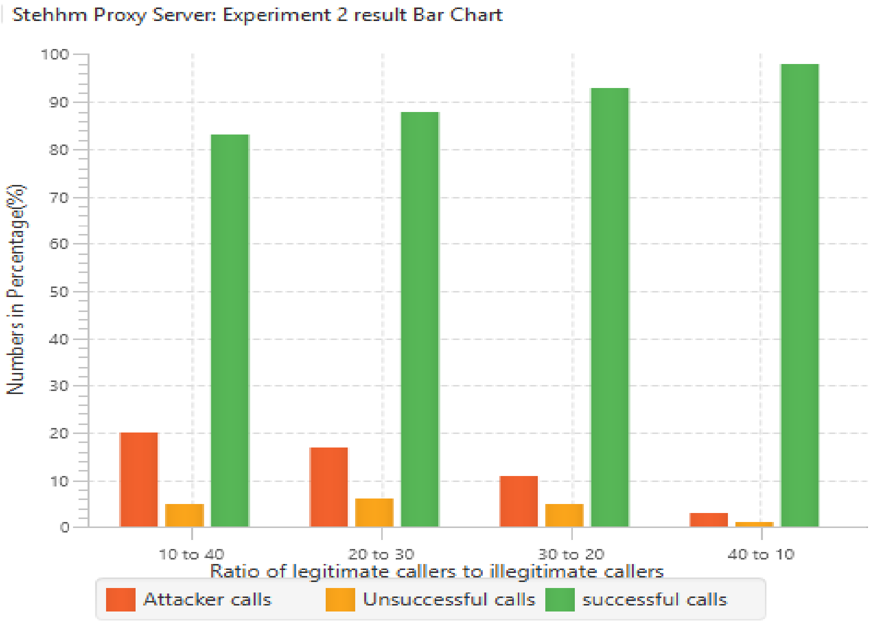


Figure 7. VoIP User Success Rate When Under CCA and Running STEHMM

The bar chart in the Figure 7 above shows that, when a VoIP server is under coordinated call attack with using and its using STEHMM as mitigation scheme, shows that 90.3% of honest users had access for the VoIP server resources. However, 8.75% of them had their calls terminated before they could complete their calls.

The bar chart in the Figure 8 below shows the experimental results of the third sets of experiment conducted to see the effect of STEHMM on VoIP networks when it is not under coordinated call attack.

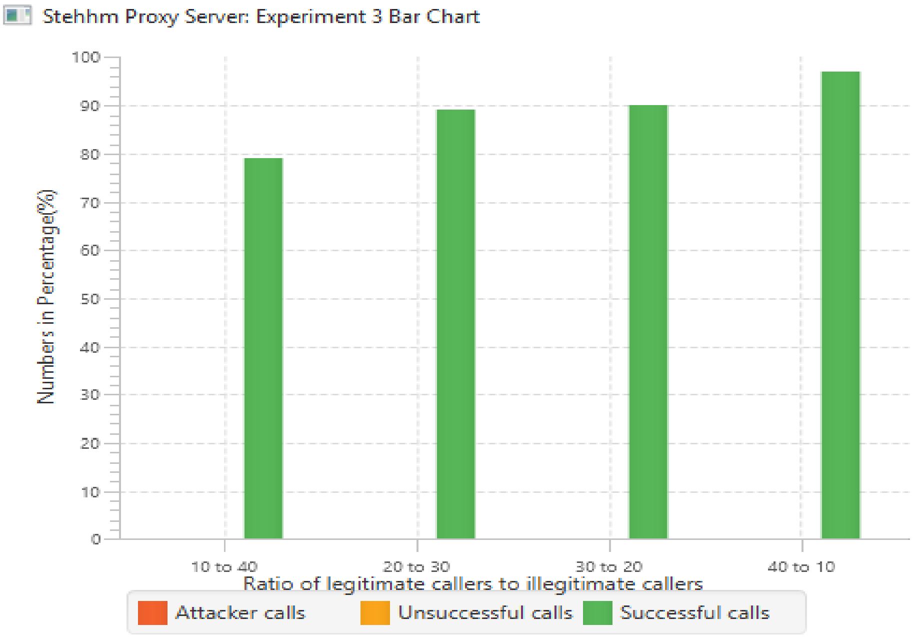


Figure 8. VoIP User Success Rate When Not Under CCA and Running STEHMM

The bar chart in the figure above shows that, when a VoIP server is not under coordinated call attack but using STEHMM as its mitigating scheme, it does not have any effect of the server resources, no unsuccessful calls.

3.1 Performance Evaluation

The performance evaluations were carefully selected considering VoIP network traffic. False Error Rate (FER), Specificity and throughput were used for performance evaluation to further prove the efficiency of STEHMM. FER was computed using the Equation 3.

$$FER = \left\{\frac{\ell_{ST}}{\mu_T}\right\} \tag{3}$$

Where ℓ_{ST} is the number honest VoIP users mistakenly identified as coordinated call attackers while μ_T is the total number of calls handled by STEHMM. Specificity was equally computed using the Equation 4.

$$Specificity = \left\{\frac{L_{ST}}{(\mu_T)}\right\} \tag{4}$$

Where L_{ST} is the total coordinated call attackers' call identified by STEHMM, while μ_T is the total number of calls handled by STEHMM. Throughput was also computed to know the effect of STEHMM on VoIP networks using the Equation 5.

$$Throughput = \frac{\alpha_{ST}}{\beta_{ST}} X\ 100 \tag{5}$$

Where α_{ST} is the total number of calls handled by STEHMM while β_{ST} is the total number of incoming VoIP calls handled by VoIP server.

The Table 5 below presents that FER test of STEHMM is 6.25% on the average of the four experiments carried out, that is, when attacker to legitimate calls are varied for 10:40, 20:30, 30:20 and 40:10 respectively. For Specificity test and Throughput, STEHMM outperformed well by 93.2%, and 3.58% respectively.

Table 5. Performance Evaluation

	FER	SPECIFICITY	THROUGHPUT
Tests	FER test (%)	Specificity test (%)	Throughput test (%)
Percentage Improvement (%)	6.25	93.2	3.58

4. Conclusion

From the results displayed it shows that without any mitigating scheme, if the VoIP server is under coordinated call attack only 15.2% of honest VoIP users had access to the VoIP system and 30.1% of them had their calls terminated before call completion. When the developed scheme STEHMM was used to mitigate coordinated call attack 90.3% honest callers had full access to the VoIP server. This signifies the mitigating scheme worked effectively. However, STEHMM is far from being perfect, for further improvement, call classification can be improved upon using source cell identification of every VoIP caller waveform and incorporating callers' classification into gold, silver and bronze users based on origin of request IP and history of users' call can improve the precision of the developed scheme.

Notation

s_i : Call interaction pattern between two parties.
ℓ_{ST} : Number honest VoIP users mistakenly identified.
μ_T : The total number of calls handled by STEHMM.
α_{ST} : Total number of calls handled by STEHMM.
β_{ST} : Total number of incoming VoIP calls.

References

[1] M. O. O. Lemos, Y. G. Dantas, I. Fonseca, V. Nigam, and G. Sampaio, "A Selective Defense for Mitigating Coordinated Call Attacks," *34th {Brazilian} {Symposium} {Computer} {Networks} {Distributed} {Systems}*, 2016.

[2] Y. G. Dantas, M. O. O. Lemos, I. E. Fonseca, and V. Nigam, "Formal Specification and Verification of a Selective Defense for TDoS Attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, Vol. 9942 LNCS, Pp. 82–97, 2016. https://doi.org/10.1007/978-3-319-44802-2_5

[3] J. Safarik and J. Slachta, "VoIP Attacks Detection Engine Based on Neural Network," *Indep. Compon. Anal. Compressive Sampling, Large Data Anal. (LDA), Neural Networks, Biosyst. Nanoeng. XIII*, Vol. 9496, Pp. 94960J, 2015. https://doi.org/10.1117/12.2178182

[4] J. Shukla and B. Sahni, "A Survey on VoIP Security Attacks and their Proposed Solutions," *Int. J. Appl. or Innov. Eng. Manag.*, Vol. 2, No. 3, Pp. 158–164, 2013. https://dx.doi.org/10.1080/19393550802308618

[5] G. Martinez, J. S. Park, A. Pescapè, Z. Wang, J. Zhan, and A. Blyth, "International Journal of Network Security," Vol. 17, No. 1, 2015.

[6] Y. G. Dantas, V. Nigam, and I. E. Fonseca, "A Selective Defense for Application Layer DDoS Attacks," *Proc. - 2014 IEEE Jt. Intell. Secur. Informatics Conf. JISIC 2014*, Pp. 75–82, 2014. https://doi.org/10.1109/JISIC.2014.21

[7] L. Amor and S. Thabet, "Deployment of VoIP Technology: QoS Concerns," *Int. J. Adv. Res. Comput. Commun. Eng.*, Vol. 2, No. 9, Pp. 3514–3521, 2013.

[8] T. G. Rahangdale, P. A. Tijare, S. NSawalkar, and S. C. O E T, "An Overview on Security Analysis of Session Initiation Protocol in VoIP Network," *Int. J. Res. Advent Technol.*, Vol. 2, No. 4, Pp. 2321–9637, 2014. https://dx.doi.org/0.1109/ICET.2014.7021022

[9] K. O. Detken and E. Eren, "VoIP Security Regarding the Open Source Software Asterisk," *Imeti 2008 Int. Multi-Conference Eng. Technol. Innov. Vol I, Proc.*, Pp. 93–98, 2008.

[10] D. Enqing, L. Guizhong, Z. Yatong, and C. Yu, "Voice Activity Detection Based On Short-Time Energy and Noise Spectrum Adaptation," *Int. Conf. Signal Process. Proceedings, ICSP*, Vol. 1, No. 1, Pp. 464–467, 2002. https://doi.org/10.1109/ICOSP.2002.1181092

[11] M. K. Mustafa, T. Allen, and K. Appiah, "A comparative Review of Dynamic Neural Networks and Hidden Markov Model Methods for Mobile On-Device Speech Recognition," *Neural Comput. Appl.*, Pp. 1–9, 2017. https://dx.doi.org/10.1007/s00521-017-3028-2

[12] A. Bietti, F. Bach, and A. Cont, "An Online Em Algorithm in Hidden (Semi-)Markov Models for Audio Segmentation and Clustering," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, Vol. 2015–Augus, Pp. 1881–1885, 2015. https://doi.org/10.1109/ICASSP.2015.7178297

[13] S. Ehlert, C. Wang, T. Magedanz, and D. Sisalem, "Specification-Based Denial-Of-Service Detection for SIP Voice-Over-IP Networks," *Proc. - 3rd Int. Conf. Internet Monit. Prot. ICIMP 2008*, Pp. 59–66, 2008. https://doi.org/10.1109/ICIMP.2008.14

[14] Z. F. Fan, J. R. Yang, and X. Y. Wan, "A SIP DoS Flooding Attack Defense Mechanism Based on Custom Weighted Fair Queue Scheduling," *2010 Int. Conf. Multimed. Technol. ICMT 2010*, Pp. 0–3, 2010. https://doi.org/10.1109/ICMULT.2010.5630386

[15] J. Tang, Y. Cheng, Y. Hao, and W. Song, "SIP Flooding Attack Detection with A Multi-Dimensional Sketch Design," *IEEE Trans. Dependable Secur. Comput.*, Vol. 11, No. 6, Pp. 582–595, 2014. https://doi.org/10.1109/TDSC.2014.2302298