

## A typical analysis of hybrid covert channel using constructive entropy analytics

Anjan Krishnamurthy Koundinya<sup>1</sup>, Gururaja Hebbur Satyanarayana<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, B. M. S. Institute of Technology and Management, Bengaluru, India

<sup>2</sup>Department of Information Science and Engineering, B. M. S. College of Engineering, Bengaluru, India

### Article Info

#### Article history:

Received May 7, 2021

Revised Mar 19, 2022

Accepted Mar 30, 2022

#### Keywords:

Channel encoding

Covert channel

Covertness index

Entropy detection

Subliminal channel

### ABSTRACT

A covert timing channel is based on modulation of the timing information in the network packets in a secured communication. The delicacy of this channel is primarily viewed as single coherent channel thwart the detection from any third-party entity or network admin. The timing covert channel is strenuous to detect under many scenarios due to the intricate complexity of the channel. The exploration of timing covert channel shed light on intrinsic design aspects which elevate understanding to an advanced level. This will effectively bring out elite literature aspects of the timing covert channel for seamless implementation. Supraliminal channels are innocuous message-based channel introduced as a trapdoor in the communication system either intentional or as vulnerability of the system. A hybrid covert channel is the existence of homogeneous or heterogeneous network covert channel variants either at same instant or at different instant of time. For instance, one of possible hybrid covert channel is the co-existence of timing covert channel in transmission control protocol (TCP) and supraliminal channel in voice over internet protocol (VoIP). This paper introduces this variant of the hybrid covert channel and their significance in network communication. The paper also refers to standard measures-entropy, covertness index to understand hybrid covert channel.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Anjan Krishnamurthy Koundinya

Department of Computer Science and Engineering, B. M. S. Institute of Technology and Management

Doddaballapur Main Road, Avalahalli, Yelahanka, Bengaluru 560064, India

Email: anjank-cse@bmsit.in, annjank2@gmail.com

## 1. INTRODUCTION

The computer network of this era is an inter-connection of compound devices with diverse capabilities. It comprises of simple computing to a very large complex computing which may have electro-mechanical parts in it. The diversity has brought about the era of internet-of-things (IoT) where everything is connected to network and controls a larger target application like smart grid, and smart traffic. The system must be driven by legitimate and formal processes to lead to a meaningful operation and outcome. The loss or malfunction of such systems leads to catastrophic effect on the eco-system or on the economy. Hence it is really very important to safeguard these systems from any malefic operations from any unknown sources. It has been seen in many cases of cyber warfare that such systems are compromised leading to attacks for ill use of systems leading to significant market loss may be worth in billions. Such attacks are implemented on any network systems through hidden messaging schemes in cryptographic methods to avoid any sort of detection by the administrative agent. The perennial use of the internet for mundane activities has imperative impact on society. Netizens may post sensitive and confidential messages without being aware of consequences. This leads to intrigued plans of victimization and non-desirable impact

to netizens. In a network interpretation, this could be significantly led to collude information leaks to unknown users of network through covert channel.

The purpose of the covert channel is to collude information secretly without the awareness of legitimate network users. The difference in the signature will indicate the presence of covert channel. A small advancement to this method is to run the entire system many number of times to match with standard signature. This is called as a statistical signature detection method. Timing covert channel [1], [2] in a secured communication can be detrimental for legitimate users as they are intricate to detect. An intricate covert timing channel [3] is designed in the protocol stack of transmission control protocol (TCP)/internet protocol (IP) by using cryptographically secure pseudo random number generators (CSPRNG). The caricature version of the packet inter-arrival time is employed in the covert timing channel [4]–[6] thus granting the covert parties to communicate in the low-profile, low-bit rate hostile environment. This behavior is clear deviation from the normal Poisson's distribution in internet traffic. A simplistic view of the covert timing channel is show in the Figure 1 which clear indicate the triggering of fabricated events to convey covert data through timing reference.

For instance, sender pulsates a shared clock at 'X' KHz constantly indicating some information to its covert receiver. Fluctuated clock pulsation is the covert encoding scheme that will be pre-shared by the covert parties. This is typical scenario in the multiprocessor-based systems which stigmatically uses uni-shared bus which eventually leads to bus-contention. An illustrative example is shown in the Figure 2. It is intractably futile to stop covert timing channel once it has made its presence in the system.

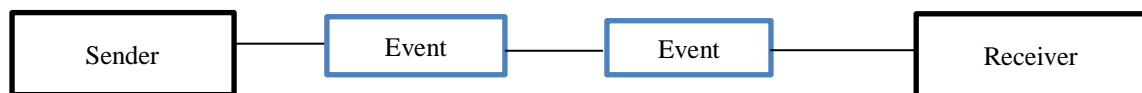


Figure 1. Simplistic view of covert timing channel

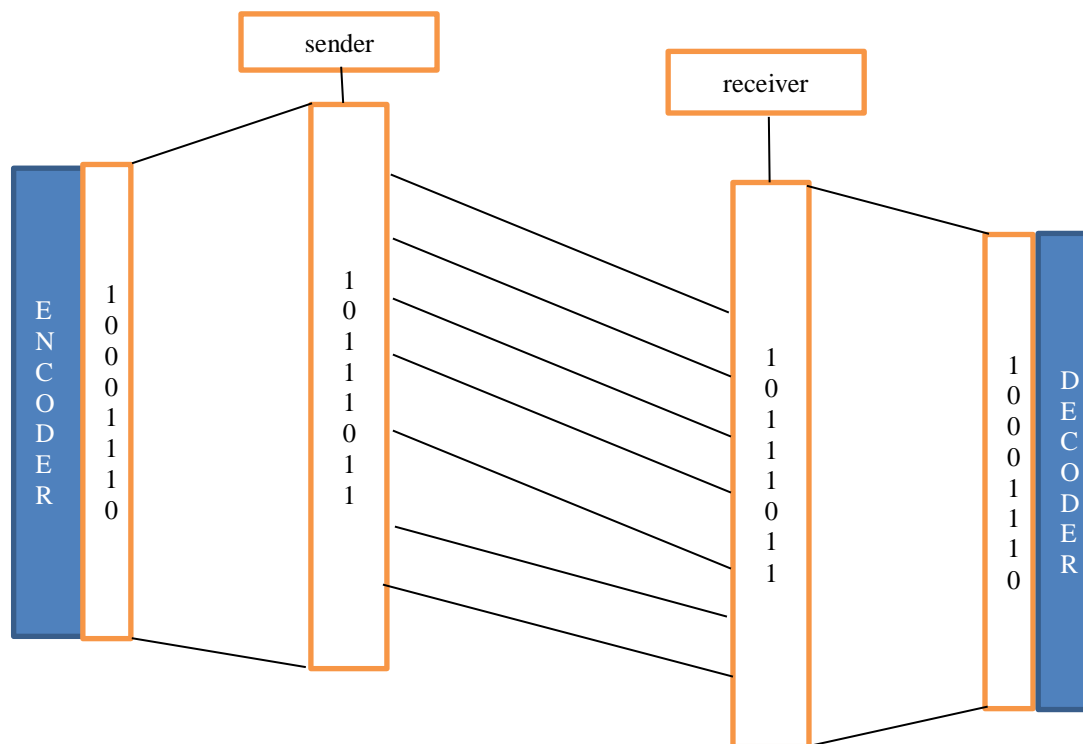


Figure 2. Example of covert timing channel

An information encoding scheme is used and shall be communicated to the other end as a bit transmission. The message is reconstructed on the other end by applying decoding scheme on the bit stream. The modulation of bit to 0 and 1 has special indication, representing transmission or no transmission, respectively. These modulated values are interpreted differently by the covert communication parties.

Timing covert channels are built by manipulation of temporal patterns of the communication networks. In fact, hidden messages are transmitted by controlling the number of events in a period of time. The capacity of covert channel is important as it deals with amount covert data that can be transmitted over the channel. The equation for capacity of covert channel is (1):

$$C = N(1 - P_d) \quad (1)$$

$N$  is the number of bits encoded in each channel symbol. The deletion probability  $P_d$  is often determined by the system design.

The subject of covert communications draws more attention, due to the advancing infrastructure of internet and attacks [7] needs an urgent focus to protect the companies/organizations from data leak and unauthorized access. If a traffic analysis is performed on the network a third part entity will be aware of the message pattern and the type of message. However in case of presence of covert channel third party entity will not be aware of hidden communication in the channel.

The covert timing channel [8], [9] will modulate the timing information by intentionally fluctuating the timing information to collude sensitive information that is undetectable by any system. Hybrid covert channel (HCC) is combination of multiple covert channels at various levels in the protocol suite seen as single cohesive covert channel at the same point of time. This channel is completely untraceable and non-detectable from any network intrusion detection systems (NIDS) or packet anomaly detection systems.

The paper visualizes an hybrid covert channel which is a special variant; A timing covert channel in the TCP and a supraliminal channel [10] in the voice over internet protocol (VoIP) protocol in the application. This variant of the multi trapdoor hybrid covert channel is completely untraceable as the covert channel established in the two different layers of the protocol stack. In many of the intrusion detection systems (IDS) system the application layer is not sniffed for any anomaly as the IDS system shall have access to the packet till the Network Layer and not beyond it. Hence it a supraliminal channel [11] in the application layer survives any detection. Similarly, the covert channel established in the TCP using the modulating events as timing channel is barely detectable in any setup of the IDS. Hence this coherent channel becomes the strongest variants of the multi-trapdoor based hybrid covert channel.

This paper proposes to detect this variant of the hybrid covert channel using constructive entropy [12] approach for each scenario of the covert channel established in various layers of the protocol stack. A differential entropy shall be calculated for entropy with covert channel and entropy without covert channel in it. This method shall further be supported by the covertness index [13], [14] which will indicate severity of the covert channelling used in this variant of the hybrid covert channel.

## 2. RESEARCH METHOD

The method of intentionally auto adjusting the inter- arrival timing of the packet sequences in IP time-replay [1] is a finest method of the communicating covert messages. The packet inter-arrival time is recorded in a normal sequence and in the covert case. This leads to anomaly in data rates and can conveniently tweak the anomaly detection schemes. A timing covert channel involves modulating the signal information very similar to that of side channel attack in such a way that manipulation effect cannot be observed. Another approach is the intricate design in the covert network timing channel with subliminal subtle issues [2] that manipulates the performance of the channel by adversely changing the regularity of the channel. This can be effective mechanism to completely disrupt communication in a legitimate network that thwarts the detection.

Jitterbugs [15] is an innovative method of inline interception to covertly send data by disruptively changing the timing of input events. Jitterbug basically resides in input device in trusted environment that colludes to leak information without vexatious on the host software system. This can be in any interactive communication application where receiver constantly monitors the traffic in the network of the sender. Simple keyboard device can be employed in such experiments. This is niche technique to extrapolate sensitive information in such application

Propose cloak [16] is an elite class of reliable timing covert channel that is fundamentally different from other channels in its design. The cloak firstly encodes message in  $N$  packets by applying uniform distribution over  $X$  flows of TCP packets. The intricate design is ideologically based on channel capacity by applying combinatorial method. This method offers ten different covert encoding schemes with unique tradeoff on channel capacity and packet marking. The packet transmissions are modulated and carefully to mimic the normal TCP flows. This method systematically addresses challenging issue in this method under various network conditions and round-trip delays.

Intricate exploration of sophisticated covert timing channel [17] is a crucial comprehension of defense against covert timing channel. The model-based covert timing channel exploits the statistical properties of network traffic to thwart detection in well-effective manner. The automated framework is based on four components: filter, analyzer, encoder, transmitter that ensure framework is light weight and effective on local area network (LAN) and wide area network (WAN) environments. The model-based covert timing channel is highly resilient and resistant against detection with minor loss in capacity. Observable traffic monitoring is a characteristic feature of the filter component in the model through analyzer. Encoder blends the cover data with the legitimate network traffic.

Jammed timing covert channel [18] is a pure delay jammer with an inclusion of the delay constraint using maximum buffer size on discrete-time packet waveforms. Fluid waveform is a class of the waveform that can be an aid in analysis. Min-max optimal jammers sought a discrete input process that mutually based on information rates. The maximum-delay-constraint (MDC) jammers with saddle-point input on continuous-time packet waveforms. The threshold of the delay is based on the jamming channel with continuous-time packet waveforms with saddle point depicting the mutual information rate. Jammers works on quantized batch departures at regular intervals on maximum-buffer-size-constrained jammers.

The timing covert channel [19] is a covert communication channel that can transfer covert data by modulating the timing behavior of an entity. The timing covert channel construction is merely based on inter-packet delays, reordering of packets, access time of the resources that is used in cryptographic programs and many more. With advent of the high- performance computing system it is possible to have varied types of covert coding schemes for seamless covert communication over high-speed network. The sophistication in build process of such channel has led to counter measures. The paper gives broad review of different process of construction of timing covert channel with covert entities. Literature presented in this paper broadly discusses about canonical applications in timing side channel, and network flow watermarking.

The detection of covert timing channel using entropy is proposed in [20] which bring the detection methods to limelight. The clandestine medium used for covert timing channel is a file or time of events. It is difficult to detect and analyze the existence of covert timing channel due to use of clandestine medium. Techniques for detection are still at infancy and merely adopt more than one approach for detection. The network is at stake when the multiple methods are involved in detection as its sores the network's bandwidth and turns to be risky process also. The paper presents novel method of using corrected conditional entropy approach for detection [21] of covert timing channel and these methods is sensitive to small change in entropy values.

Network based intruders seldom attack [22] are conducted on own host using identity concealment of the origin also known as "stepping stones". The attackers are completely not traceable in this approach due to the stepping stones and require correlations with connections. The time-based approach is aplomb in its capability and to thwart the detection. The paper proposes and model on watermark-based correlation scheme that is designed intricately against timing perturbations. The introduction of the watermark is by adjusting the timing of the chosen packet in the flow. With the help of the redundancy techniques, it is possible to robust and resilient system that inherently limits the uniquely distributed and independent random time perturbation over longer flows. This is significant tradeoff between the time perturbation and achievable correlation effectiveness. The experiment showcased in this work is confidently better than existing, non- active time-based correlations.

A formidable approach of using timing information of the packet for covert communication [23] is used in the several schemes like watermarking and network timing covert channels. Majority of these schemes embed the covert data in the inter-packet delay. The detection of such schemes is based on analyzing the perturbed traffic pattern, degraded jitter, packet loss, and packet reordering events. TCPScript method address the shortcomings of the normal covert schemes by embedding the covert data in the normal TCP data bursts. This reduces the analysis of the perturbation of the timing and packet loss.

A paper on detection hybrid covert channel with covert channel in TCP and subliminal channel in the SSL is proposed and detected in the work [13] and is the motivation to detect other possible variants of the hybrid covert channel. The approach mentioned in the work is using the packet sniffing and lateral detection in a forensics way. However, the approach is not on live wire with real time detection.

## 2.1. Proposed method

The entropy rate [13], [24], [25] can be easy measure to check the presence of covert channel in communication channel. The entropy in channel is measure of complexity or regularity in the channel. As per the Shannon's entropy theory, the channel capacity is derived from the entropy which represents the number of the characters symbols that can be pushed in a transmission line. The entropy can also serve a measure of the uncertainty of the random variable. The entropy rate is directly related to the covertness index [26] for a covert channel with multiple clandestine mediums.

Entropy rate is measured as conditional entropy for infinite string length. Conditional entropy can be of first order entropy if the entropy rate belongs to the first order probability density function. A complex process will have higher entropy rate that will be less than the first order entropy. The conditional entropy is defined as shown in (2).

$$H(X_1, \dots, X_m) = - \sum_{x_1 \dots x_m} P(x_1 \dots x_m) \log P(x_1 \dots x_m) \quad (2)$$

The entropy rate for different message will be different and is dependent on frequency of occurrence of the letter and the value of the  $H(X) < 3$  for all messages. For example, to send the message “network” the entropy value will be  $H(X)=2.803$ , inferring the fact the 3 bits are required for transmission for this. In general, for all network transmission the maximum cap on the entropy rate of the first order will be three times  $X$ .

$$H(X) = 3 * |X| \quad (3)$$

First order entropy will be always be less than the number of the bits of that protocol header field ( $B_f$ ). A covert channel will tap in this and make use of the protocol fields to embed the covert data. i.e.,  $H(X) < | \text{Maximum number of bits in that field } (B_f) |$

For instance, the VoIP sender or receiver ID field can be used for covert data can use 16 bits in the IP header, so to send the message “network” which basically requires minimum of 21 bits. Hence this will adversely affect the channel capacity of the legitimate communication channel and will boost the capacity of the covert channel. The covert channel capacity for this instance will be:

$$C_c = \log_2(1 + 16) = 0.25$$

This infers that 25% of the total bandwidth channel will be used for covert purpose only thus reducing legitimate channel capacity by 25%. This change will have nil effect on the quality of service (QoS) parameters, appearing as if the packet is normal for communication. Thus, this leads to untraceable covert communication that can thwart any kind of anomaly detection methods employed in the NIDS.

### 3. RESULTS AND DISCUSSION

The prime focus of the analysis shall be on two important metrics as they will provide the intricate complexity in the detection and formation for such hybrid covert channel visualized: i) entropy for each scenario and ii) covertness index for each channel type. The covertness index for a covert channel is the measure of detectability of the channel for any IDS or anomaly detection software embedded in network devices. The value of 0.5 and above of the covertness index shall indicate the channel is very covert and hard for detection. This is exactly the case in the hybrid covert channel visualized in this paper where the application software may fail to detect the activity in the VoIP and in TCP. The supraliminal channel in the VoIP is very hard for detection and combining data encoding in the covert channel in TCP would be too hard to detect. Further, the analysis made with respect to entropy and covertness index [13], [14] is given in Table 1 and graph for the same is shown in Figure 3 for a supraliminal channel in application layer.

Table 1. Multi-trapdoor analysis of VoIP

Sl. No.	Trapdoor Name	No. of Trapdoors	No. of Trapdoors used	Algorithm	Covertness Index	Entropy	C/E
1	Supraliminal Channel-VoIP-Single	5	1	NIL	0.2	2.903	0.094
2	Supraliminal Channel-VoIP-dual	5	2	NIL	0.4	5.706	0.22
3	Supraliminal Channel-VoIP-triple	5	3	NIL	0.6	11.41	0.45

The entropy for the TCP is based on the trapdoors inserted in the protocol suite and various points in the TCP header it is possible to add covert data. These are covert vulnerable fields. The Figure 4 depicts the compassion of covertness index over the trapdoors set. The steep increase in the entropy value amounts to the formation of covert channel that is capable for detection.

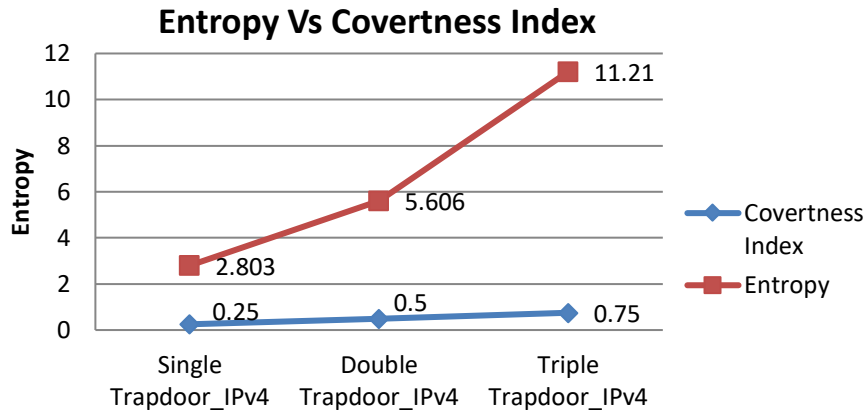


Figure 3. Entropy vs covertness index for VoIP

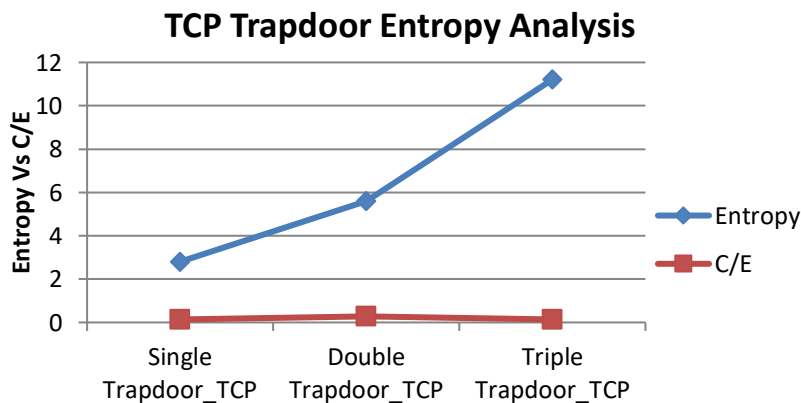


Figure 4. Entropy vs covertness index in covert channel based on TCP

#### 4. CONCLUSION

It is significant to note that timing covert channel is most powerful and resilient channel over all its category of covert channel. Entropy based analysis shed a light over the analyzing the composition of the covert timing channel. In jest, there are ample opportunities to explore more research work in the unknown space of the covert timing channel. Further study can be on combination of timing covert channel and subliminal channel in cryptographic protocol. The time related analysis place important role in the decryption algorithm.

#### ACKNOWLEDGEMENTS

Author would like to thank Late Dr. V K Ananthashayana, Former Head, Dept. of CSE, MSRIT, Bengaluru, India and Late Prof. M S Sudhi, Former Head, Dept. of ECE, MSRIT, Bengaluru, India for igniting passion for research.




#### REFERENCES

- [1] S. Cabuk, "Network covert channels: design, analysis, detection, and elimination," Spafford, Purdue University, 2006.
- [2] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels," in *Proceedings of the 11th ACM conference on Computer and communications security - CCS '04*, 2004, p. 178, doi: 10.1145/1030083.1030108.
- [3] X. Luo, E. W. W. Chan, and R. K. C. Chang, "Cloak: A Ten-Fold Way for Reliable Covert Communications," in *12th European Symposium On Research In Computer Security*, 2007, pp. 283–298, doi: 10.1007/978-3-540-74835-9\_19.
- [4] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: automated modeling and evasion," in *Recent Advances in Intrusion Detection*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 211–230.
- [5] J. Giles and B. Hajek, "An information-theoretic and game-theoretic study of timing channels," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2455–2477, Sep. 2002, doi: 10.1109/TIT.2002.801405.
- [6] A. K. Biswas, D. Ghosal, and S. Nagaraja, "A survey of timing channels and countermeasures," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–39, Jan. 2018, doi: 10.1145/3023872.




- [7] B. D. Naik, S. C. Boddukolu, P. Sujatha, and P. Dhavachelvan, "Connecting entropy-based detection methods and entropy to detect covert timing channels," *Advances in Intelligent Systems and Computing*, vol. 176, pp. 279–288, 2012, doi: 10.1007/978-3-642-31513-8\_29.
- [8] X. Wang and D. S. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays," 2003, doi: 10.1145/948109.948115.
- [9] C. Sanders, J. Valletta, B. Yuan, D. Johnson, and P. Lutz, "Employing Entropy in the detection and monitoring of network covert channels," in *The 2012 International Conference on Security and Management*, 2012, pp. 1–5.
- [10] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44–57, 2007, doi: 10.1109/COMST.2007.4317620.
- [11] R. A. Kemmerer, "A practical approach to identifying storage and timing channels: twenty years later," in *18th Annual Computer Security Applications Conference, 2002. Proceedings*, 1982, pp. 109–118, doi: 10.1109/CSAC.2002.1176284.
- [12] X. Luo, E. W. W. Chan, and R. K. C. Chang, "TCP covert timing channels: Design and detection," in *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, 2008, pp. 420–429, doi: 10.1109/DSN.2008.4630112.
- [13] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *IMC '05: Proceedings of the 5th ACM SIGCOMM conference on Internet measurement*, 2005.
- [14] A. K. S. N.K., and J. Abraham, "Entropy based detection and behavioral analysis of hybrid covert channel in secured communication," *International Journal of Network Security & Its Applications*, vol. 7, no. 3, pp. 39–53, May 2015, doi: 10.5121/ijnsa.2015.7304.
- [15] K. Anjan and J. Abraham, "Behavioral analysis of transport layer based hybrid covert channel," in *Third International Conference, CNSA 2010*, 2010, pp. 83–92, doi: 10.1007/978-3-642-14478-3\_9.
- [16] E. Li and S. Craver, "A supraliminal channel in a wireless phone application," in *Proceedings of the 11th ACM workshop on Multimedia and security - MM&Sec '09*, 2009, p. 151, doi: 10.1145/1597817.1597843.
- [17] S. Craver, E. Li, J. Yu, and I. Atakli, "A supraliminal channel in a video conferencing application," in *Information Hiding: 10th International Workshop*, 2008, pp. 283–293, doi: 10.1007/978-3-540-88961-8\_20.
- [18] D. Stefan, A. Russo, P. Buiras, A. Levy, J. C. Mitchell, and D. Mazières, "Addressing covert termination and timing channels in concurrent information flow systems," *ACM SIGPLAN Notices*, vol. 47, no. 9, pp. 201–214, Oct. 2012, doi: 10.1145/2398856.2364557.
- [19] V. Gorodetski and I. Kottenko, "Attacks against computer network: formal grammar-based framework and simulation tool," in *Proceedings of the 5th international conference on Recent advances in intrusion detection*, 2002, pp. 219–238.
- [20] M. Handley, V. Paxson, and C. Kreibich, "Network intrusion detection: evasion, traffic normalization, and end-to-end protocol semantics," in *Proc. 10th USENIX Security Symposium*, 2001, vol. 10, pp. 115–131.
- [21] L. Kozłowski "Description of the Entropy calculation," Shannon entropy calculator, <http://www.shannonentropy.netmark.pl/> (Accessed: May 16, 2021)
- [22] T. Sohn, J. Seo, and J. Moon, "A study on the covert channel detection of TCP/IP header using support vector machine," in *Lecture Notes in Computer Science*, 2003, pp. 313–324.
- [23] R. M. Stillman, "Detecting IP covert timing channels by correlating packet timing with memory content," in *IEEE SoutheastCon 2008*, Apr. 2008, pp. 204–209, doi: 10.1109/SECON.2008.4494286.
- [24] S. H. Sellke, C.-C. Wang, S. Bagchi, and N. Shroff, "TCP/IP timing channels: theory to implementation," in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, Apr. 2009, pp. 2204–2212, doi: 10.1109/INFCOM.2009.5062145.
- [25] I. S. Moskowitz and A. R. Miller, "The channel capacity of a certain noisy timing channel," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1339–1344, Jul. 1992, doi: 10.1109/18.144712.
- [26] H. S. Gururaja, M. Seetha, and A. K. Koundinya, "Covert analysis of subliminal channels in legitimate communication," in *Lecture Notes in Computer Science*, 2012, pp. 583–592.

## BIOGRAPHIES OF AUTHORS



**Anjan Krishnamurthy Koundinya**    has received his B.E (CSE), M.Tech (CSE), and Ph.D degree from Visveswariah Technological University (VTU), Belagavi, India. He has been awarded Best Performer PG 2010, First Rank Holder (M. Tech CSE 2010) and recipient of Best Ph.D Thesis Award by BITES, Karnataka for the academic year 2016-17. He has served in industry and academia in various capacities for more than a decade. He is currently working as Associate Professor and PG Coordinator in Dept. of CSE, BMSIT&M, Bengaluru, India. Email: annjank2@gmail.com.



**Gururaja Hebbur Satyanarayana**    obtained his B.E. in Computer Science and Engineering and M. Tech in Computer Network Engineering from VTU, Belgaum. He is pursuing his doctoral research in the area of Network Security from JNTU, Hyderabad. He has around 15 years of teaching experience and has been awarded as Best Teacher in his previous workplace. He has been certified as a top performer for Mentoring Educators in Educational Technology by IIT-Bombay. He is currently working as an Assistant Professor in the Department of Information Science and Engineering, B.M.S. College of Engineering (BMSCE), Bengaluru. Email: gururaja.hs@gmail.com.