SCMS SCHOOL OF ENGINEERING AND TECHNOLOGY,KARUKUTTY

BOOKS/CONFERENCE INDEX 2021-2022

3.3.2 Number of books and chapters in edited volumes/books published and papers published in national/ international conference proceedings per teacher during 2021-2022

Sl. No.	Name of the teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Calendar Year of publication	ISBN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
1	Dr.Akhila M		Bio-reactor Landfill for Sustainable Waste Management – A Review		2021 National Conference on Sustainable Practices in Civil Engineering	National	Oct,2021	ISBN:978-93-5493-715-6	SCMS School of Engineering and Technology, Ernakulam, India	
2	Dr. Gibin George	2D Nano MaterialsChemistry and Properties	Effect of Exfoliation on structural and electrochemical properties				May 2022	9781003178453	SCMS School of Engineering and Technology, Ernakulam, India	CRC Press
3	Litty Koshy	Algorithms for Intelligent Systems book series (AIS)	Underwater Image Enhancement Using Fusion Stretch Method.	Algorithms for Intelligent Systems book series (AIS)	Machine Intelligence and Smart Systems	International	May,2022	978-981-16-9649-7	SCMS School of Engineering and Technology, Ernakulam, India	Springer, Singapore
4	Litty Koshy	2021 Smart Technologies, Communication and Robotics (STCR)	Video Forgery Detection using CNN	IEEE Xplore			Nov,2021	978-1-6654-1806-5	SCMS School of Engineering and Technology, Ernakulam, India	IEEE
5	Dhanya K A	Securing Social Networks in Cyberspace	A Deep Learning-Based Model for an Efficient Hate-Speech Detection in Twitter.				2021	9781003134527	SCMS School of Engineering and Technology, Ernakulam, India	CRC PRESS
6	Dr. Sonal Ayyappan		Age and Spoof Detection from Fingerprints using Transfer Learning	IEEE Xplore	2021 International Conference on Advances in Computing and Communications (ICACC)	International	Feb, 2022	978-1-6654-3919-0	SCMS School of Engineering and Technology, Ernakulam, India	IEEE
7	Josna Philomina		A study on the Effect of Hardware Trojans in the performance of Network on chip Architectures	IEEE Xplore	2021 8th International Conference on Smart Computing and Communications (ICSCC)	International	September,2021	978-1-7281-9687-9	SCMS School of Engineering and Technology, Ernakulam, India	IEEE
8	Asha S		Downsampling Attack on Automatic Speaker Authentication System	IEEE Xplore	2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA)	International	Dec,2021	978-1-6654-0969-8	SCMS School of Engineering and Technology, Ernakulam, India	IEEE
9	Deepasree Varma		Analysing Gender and Age aspects of cyberbullying through online social media	IEEE Xplore	2021 International Conference on Advances in Computing and Communications (ICACC)	International	Feb,2022	978-1-6654-3919-0	SCMS School of Engineering and Technology, Ernakulam, India	IEEE

10	Jency Rena		Excavation of Time sliced and Cost based KDD for the lead generation and promotion on B2C/B2B Sales	IEEE XPLORE	2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)	International	June, 2021	978-1-6654-0521-8	SCMS School of Engineering and Technology, Ernakulam, India	IEEE
11	Rosebell Paul , Neenu Sebastian	Computer Networks, Big Data and IoT	Study on data transmission using Li-Fi in Vehicle to Vehicle Anticollision system		Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 66)		June,2021	978-981-16-0965-7	SCMS School of Engineering and Technology, Ernakulam, India	Springer Link
12	Blessy Antony	Computer Networks, Big Data and IoT	Analysis of Sybil Attacks in Online Social Networks		Lecture Notes in Networks and Systems book series (LNNS, volume 197)		June,2021	978-981-16-0980-0	SCMS School of Engineering and Technology, Ernakulam, India	Springer Link
Total number of books and chapters in edited volumes/books published and papers published in national/ international conference proceedings per teacher during 2021-2022										**12**

SCMS SCHOOL OF ENGINEERING & TECHNOLOGY
KARUKUTTY
ERNAKULAM
683 576

PRINCIPAL
SCMS SCHOOL OF ENGINEERING & TECHNOLOGY
VIDYANAGAR, PALLISSERY, KARUKUTTY
ERNAKULAM, KERALA-683 576

Analysis of Sybil Attacks in Online Social Networks Using SyPy

Christina Roseline, Blessy Antony, Bijitha Balakrishnan, Chaithra C. V., and P. V. Bhavyasree

Abstract Sybil attacks in online social networks have crucial security implications. The problem of pernicious activities in these networks, such as Sybil attacks and use of bogus identities, can severely affect the social activities in which users interact. Hence, these types of spiteful accounts must be observed and deactivated. In this paper, we simulate an online social network with an honest region and a Sybil region. This paper mainly focuses on the various parameters in the online social network and scrutinizing the impact of these parameters on Sybil attack. It is equally important to detect the most vulnerable nodes in the network to avert them from malicious users. This paper requires extensive knowledge about graphs and its properties are probability triads, clustering coefficient, degree distribution, etc.

Keywords Sybil attacks · Graph based · Vulnerable nodes · Degree distribution

1 Introduction

Widening of online social networks (OSNs), for example, Twitter, Facebook, and YouTube, has changed the manners by which individuals associate, think, and lead business. Recently, people have encapsulated tremendous action via Web-based media destinations, bringing about an extraordinary measure of client produced content at a persistent movement. The tremendous amount of users on OSNs has made them the greatest wellspring of solid character administrations for the Internet. As the ubiquity and utilization of OSNs have expanded, the incitement to assault these frameworks have likewise developed. A malevolent client makes different counterfeit characters to get admittance to significant private data to perform different sorts of cybercrimes like trading off information honesty, "savaging" that is making purposely provocative or analysis of feelings or hostile online postings, misleading, fixing notoriety, and violating trust in online affiliations. These attacks are types of Sybil attacks [1]. Sybil attack derives from the book Sybil that emphasizes a case study concerning a woman called Sybil Dorset who was treated with multiple identity disorder [1].

C. Roseline (✉) · B. Antony · B. Balakrishnan · Chaithra C. V. · P. V. Bhavyasree
SCMS Engineering and Technology, Ernakulam, Kerala, India

V. Bhateja et al. (eds.), *Computer Communication, Networking and IoT*, Lecture Notes in Networks and Systems 197, https://doi.org/10.1007/978-981-16-0980-0_16

OSNs have become an essential aspect of our everyday life, with numerous individuals totally depending on them in the domain of work, social communications, data sharing, and different parts of day-by-day living [2]. Any depressing impact on these zones because of the assaults harms the client experience and furthermore the respectability and security of the given organization. They are made as open stages. To horrendous clients, the most captivating some portion of OSNs is that they can be promptly associated with numerous clients at an attainable expense in contrast with other Web channels. Another major OSN proviso is that online clients will in general confide in their social associations and aimlessly esteem them. In this way, they may fall into a snare set by counterfeit social associations submitted by digital aggressors.

Different explores have indicated that nearly every individual who has invested some energy in Twitter and Facebook has interacted with bogus profiles. In actuality, 1 out of 20 user accounts on Twitter is believed to be Sybil, while on Facebook, somewhat more than 1 of every 100 dynamic users are bogus personalities [3]. The Sybil accounts are typically run by low-paid people or even via computerized bots with the point of swelling devotees, pushing spam or malware and in any event, impacting public talk. The fascinating piece is that Sybil accounts are very simple to get on the Web. The utilization of these records to make social help and to impact genuine clients is raising. A genuine model can be found in a recent report on 12 million clients of Weibo—a Chinese informal community like Twitter. This examination found that up to million clients partook in crusades that hoped to impact clients on items and administrations. The greater part of them engendered messages and referenced items and administrations from certain persuasive records—prone to be the brand behind these records. Sybil assault will undoubtedly get a lot greater and more extensive in the coming years, as informal communities become much more firmly combined with individual spending. In other words, users might need to be cautious previously tolerating any new companion demands, as the underground market in purchasing and selling counterfeit records will undoubtedly get considerably greater. Hence, it is very much essential to detect and eradicate all the Sybil accounts from online social networks.

In general, the Sybil detection [4] schemes are divided into four main categories:

- Graph-based schemes
- Machine learning-based schemes
- Manual verification
- Prevention approaches

In this project, we make use of graph-based methods [4]. Graph-based methods with the employment of social network information, represent interdependencies between objects using edges or links, within the case of Sybil. These techniques emphatically rely on social chart properties to distinguish Sybil clients from real clients [5]. Inside the social graph, Sybil and honest region exist, and furthermore the associations between them are free, as appeared in Fig. 1.

In our work, using graph-based methods, we initially simulate an online social network and then analyze the various parameters in this network which can have a

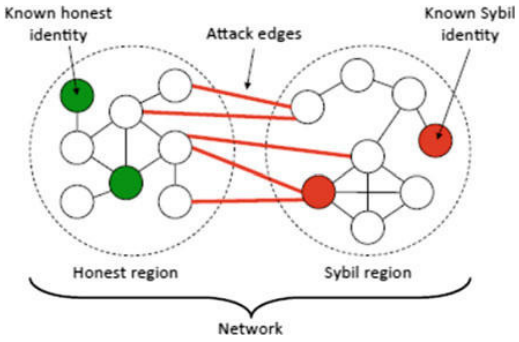


Fig. 1 Honest and Sybil region

great impact on Sybil attacks. This paper also makes use of SyPy module which is an easy-to-use Python package for Sybil node detection in social and information networks. Using this simulated network and with the utilization of SyPy Python package, we could efficiently determine how Sybil attacks can accelerate and decelerate with modification in these parameters. Once the impact of different parameters on Sybil attack is identified, the users vulnerable to these attacks can be detected effortlessly in real life.

This paper is sorted out as follows: Sect. 2 provides the related work of this topic; Sect. 3 provides the overview of the system architecture; Sect. 4 discusses the experiments and results; and Sect. 5 concludes the paper.

2 Related Works

Graph-based Sybil detection [4] has gained greatest attention in today's world. In graph-based Sybil detection, Y. Boshmaf in 2013 proposed a unified framework for evaluation and analysis of machine learning algorithms. The changes made over graphs are analyzed continuously and local communities are identified by making use of graph-based Sybil detection (GSD) [6]. Here, different models are stipulated to analyze, configure, design, implement, and assess the existing graph-based Sybil detection algorithms. Many of the real-world algorithms are evaluated and in such a way Facebook is analyzed to take up the necessities of designing and analysis of algorithms. This model basically focuses on open online social networks. Facebook, Twitter, Dropbox, etc., are the examples of such online social networks (OSNs). In OSNs, the user identification and their liaisons are prototyped as graphs. A graph $G = (V, E)$, where every node $u \in V$ represents a user identity and every edge $e = (u, v) \in E$ represents a relationship between two identities. GSD algorithms are handled by finding communities around known honest nodes [3]. There are basically two communities: global or local community detection. The global community detection is done by using Girvan and Newman algorithm [7], and the local community

detection is done by Andersen, Chung, and Lang algorithms [8]. This paper enables the analysis and design of the existing and the new GSD algorithms that provides security and privacy that can be easily evaluated empirically.

The use of trust relationships, such as social links, to counter undesirable communication is one of the major threats pointed by fake accounts. Ostra [9], proposed by Mislove et al. in 2008, delves into this concern. Ostra limits the total amount of undesirable connection a user can create that is based on the number of social links the user has. It then relies on the matter that it is challenging for a malicious user to create arbitrarily many such trust relationships. Here, a method is explained that can exploit the already existing trust relationships between users to impose a cost on the senders of unwanted communication in a way that avoids the drawbacks of existing solutions. This system depends on extending trust relationships to link senders and receivers through chains of pairwise trust relationships. It then uses a pairwise, link-based credit scheme that imposes a cost on originators of undesirable communications without demanding any sender authentication or global identities. The system also relies on criticisms and ideas from receivers to distinguish unwanted communication. Any user who still wishes to continue sending such communication risks isolation and eventually loses the ability to communicate. This system can make use of such existing social links because achieving and maintaining a relationship often demands some effort. With respect to Ostra, this property of a social network ensures that an attacker cannot achieve and maintain randomly many relationships or replace the lost relationships effortlessly. Ostra is widely applicable. It is suitable for both content-sharing systems like YouTube as well as messaging systems such as e-mail.

Integro [10] proposed by Boshmaf in 2008 is a scalable defense system that helps online social networks (OSNs) to detect automated fake accounts using a robust user ranking scheme. Integro is mainly designed for the social networks whose social relationships are bidirectional and whose ranking processes are fully transparent to the users. It starts with estimation of the accounts of the victim's user-level activity like gender, time, number of friends, which are cheap to extract from the user, since the last update. These are extracted from the user in order to train the classifier to predict the unknown labels in an online social network. After the activities of a user is detected, Integro combines these predictions into graphs as their weights so that the edges incident to predicted victims have much lower weights than the others. At last, it lists user accounts based on a modified random walk [11] that starts from the real account. Integro also guarantees that most of the real accounts ranks higher [2] than fake accounts so that the OSN operators can take actions against the low-ranking fake accounts. In Integro, as victims are directly connected to the fake accounts, they form a border line [12] separating real accounts from the fake accounts in an online social network. Based on the landing probability of the modified random walk that begins from a real known account, it also ranks the user accounts. Integro achieves linear scalability with the number of nodes in a graph. Integro computationally practical even for large OSNs such as Facebook [13] and Tuenti as it thwarts fakes in the wild with at least 10 times more precision.

GANG [14], proposed by Wang et al. in 2017, is a guilt-by-association technique that is utilized in coordinated charts, to perceive misrepresentation clients in OSNs. In GANG, a parallel irregular variable is related with every client and a mark is allocated, and afterward a novel pairwise Markov random field (pMRF) [11] is designed to model the probability distribution of all the random variables based on the directed social graph. This pMRF assimilates unique characteristics of the fraud users detection problem. The pMRF produces a larger joint probability, if two users in a graph have the same label and are linked by bidirectional edges. But if u and v are linked by a unidirectional edge (u, v), and if u is fraudulent or v is normal or vice versa, then whether the unidirectional edge (u, v), does not influence the joint probability of pMRF and this can be because of the fact that a malicious user can follow any other users without being followed back, whereas a honest user can be followed by any other users without following them back. In GANG, to measure the posterior probability distribution for each binary random variable, loopy belief propagation (LBP) is used [15] and for the corresponding user, it is used to predict the label. But there were many problems with the basic version [15]. Therefore, the later versions of GANG are optimized in such a way that it includes removing message maintenance and estimating GANG as a concise matrix form. The later versions of GANG are also evaluated and compared with various existing guilt-by-association methods using a large-scale Twitter dataset and a large-scale Sina Weibo dataset. Both datasets have labeled fraudulent and normal nodes and have directed edges. Results additionally exhibit that GANG outperforms existing guilt-by-association methods.

3 Architecture

The proposed architecture is shown in Fig. 2. The social network is defined by a graph $G = (V, E)$ consisting of a set of vertices V, denoting the user accounts on the social network and E, a set of edges, that corresponds to the social relationships between users. A bidirectional relationship exists between edges and is incarnated with an undirected edge denoting that two nodes trust each other. The subgraph of G consists of two regions—honest region and the Sybil region. The honest region contains honest nodes and the Sybil region contains the Sybil nodes in the network.

The network consists of two kinds of nodes—the honest nodes and the Sybil nodes. The honest nodes are the benign users in the network, some of the honest nodes are considered to be known nodes/labels. The honest users that accept the friend requests from the malicious users are said to be the victim nodes. The Sybil nodes are the bogus identities in the network that perform various adversarial activities in the network like stealing the user data, spreading the misinformation and even distributing the malware.

There are also three different kinds of edges—honest edges, Sybil edges, and the attack edges. The honest edges are the edges that connect the honest nodes with each other. The Sybil edges are the edges that connect the Sybil nodes with each other. The edge that connects the Sybil node in the Sybil region and the honest node in the

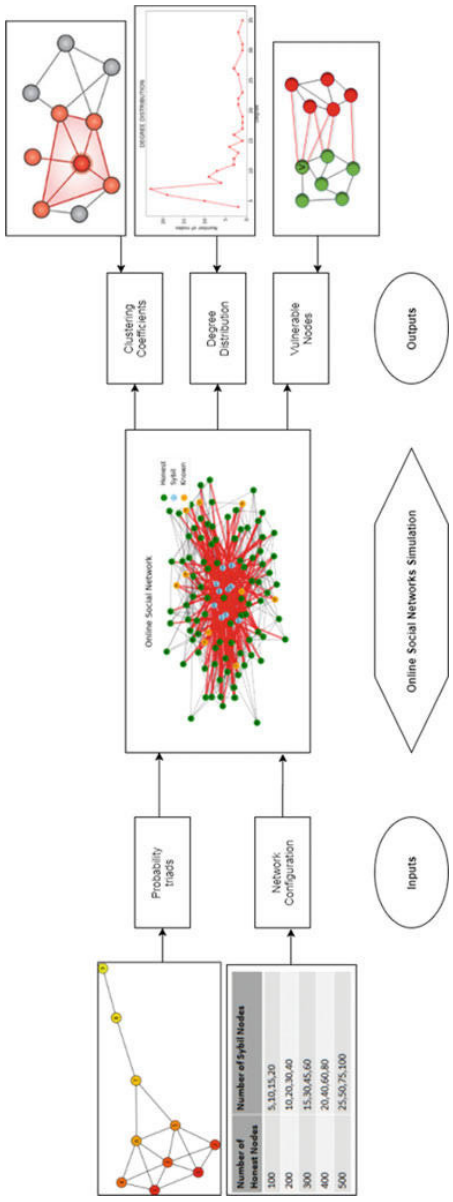


Fig. 2 Proposed architecture

honest region is the attack edge, that is the attack edges create a connection between these two regions.

Our mechanism uses a Python package SyPy for the simulation and the analysis of the network. It is built around the three assumptions:

1. The honest region is fast mixing, that is it is well connected.
2. The defender knows at least one honest node.
3. The network structure consists of two regions—Sybil region and the honest region.

Our model works in two steps. The process starts with a network simulation. In the first step we create a network consisting of honest nodes, Sybil nodes, some known labels and randomly stitches the attack edges between them. Both the honest and Sybil regions are connected by attack edges between them. In the second step, a performance analysis is done on the above simulated network. This can be performed by varying the various parameters in the simulated network which incorporates the network configuration and also the probability of forming triads to determine the vulnerable nodes and the clustering coefficient, respectively.

3.1 Network Simulation

The network simulation deals with the creation of both the Sybil and also the honest regions. The regions are created using power law graph functions included within the network.

Power Law Graphs

In the power law graph, most nodes have a relatively low level of connectivity, but a few nodes will have a high degree of connectivity. The nodes with the large degree form the hubs in the network. The existence of hubs will give the degree distribution a long tail (Fig. 3).

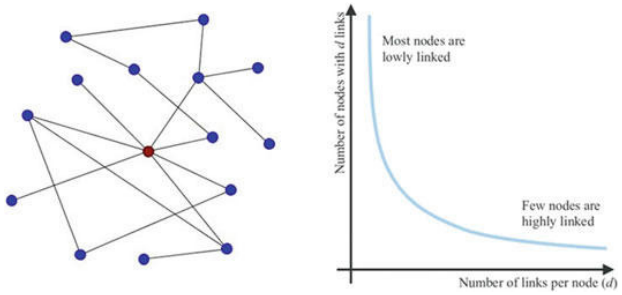


Fig. 3 Power law graph

Table 1 Different network configurations

Number of honest nodes	Number of Sybil nodes
100	5, 10, 15, 20
200	10, 20, 30, 40
300	15, 30, 45, 60
400	20, 40, 60, 80
500	25, 50, 75, 100

After the regions are created, we randomly stitch the attack edges between these two regions. It is done by randomly picking one node from each of the two regions and stitching edges between these two regions.

3.2 Vulnerable Nodes Detection

The most vulnerable nodes in the network are found out. Vulnerable nodes are more likely to be the victims than others. They are the honest nodes that have more number of connections with the Sybils and are more sensitive to Sybil attacks. We then make variations in the network configuration.

Configurations used for detecting the vulnerable nodes in various iterations are as follows:

From Table 1, it is clearly visible that for the given number of honest nodes, its 5, 10, 15, and 20% of Sybil nodes will be used in the various iterations.

3.3 Determining Clustering Coefficient

A clustering coefficient is the degree to which nodes in a graph tend to form a cluster. In simple words, it is said to be the extent to which one's friends are also friends of each other.

Clustering coefficient is given by the equation:

$$\begin{aligned} \text{Clustering coefficient} &= \frac{\text{Number of triads formed}}{\text{Total no. of triads possible}} \\ &= \frac{2T(u)}{\deg(u)\deg(u-1)} \end{aligned} \tag{1}$$

Clustering coefficient for node u can also be defined as the fraction of possible triangles that exist for the node u. In Eq. (1), $T(u)$ is the triangles through u and $\deg(u)$ is the degree of the node u. Clustering coefficient is determined by varying the probability triads.

Probability Triads

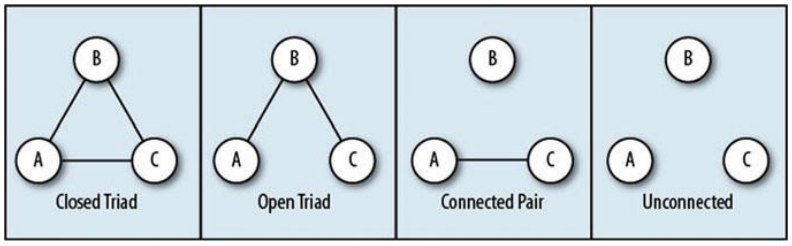


Fig. 4 Four possible triadic states in a graph

Probability triad is the probability of adding a triangle between the node connections. It can be defined as the property among the three nodes *A*, *B* and *C* such that if a strong relation exists between *A* and *B* and also between *B* and *C*, then there is a probability of a strong relation between *A* and *C* (Fig. 4).

3.4 Degree Distribution

The degree of a node in a network is the number of connections it has to other nodes and the degree distribution is the fraction of vertices with a particular degree. It describes a relationship between the degree of a node and its frequency of occurrence. Most of the real-world networks exhibit power law degree distribution, that is there are few nodes with higher degree and many nodes with very less degree.

4 Experiments and Results

This is the visualization of our simulated graph. We simulated our graph with the base configuration being 100 honest nodes represented by green color, 10 Sybil nodes represented by blue and we randomly selected 10 known honest nodes represented in yellow. The attack edges are in red color and honest connections are in black color (Fig. 5).

4.1 Vulnerable Nodes

Vulnerable nodes in the various iteration are determined in the graphs given in Fig. 6.

We have inferred from the above graphs, when the number of Sybils are increased, simultaneously the vulnerable nodes are also increased.

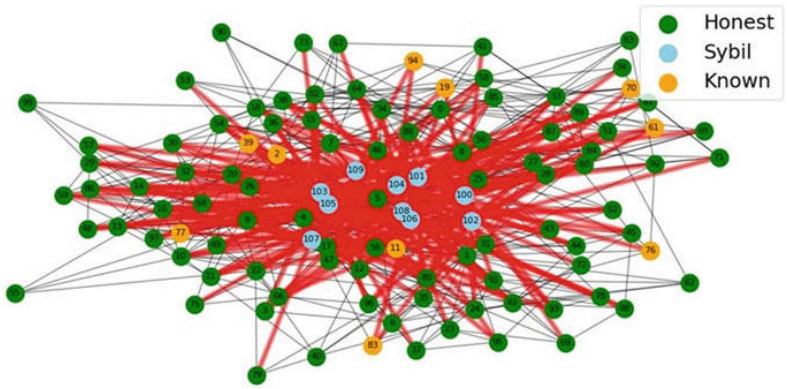


Fig. 5 A simulated online social network

Exception: In Fig. 6a, we have observed that when the number of honest nodes is 100 and the number of Sybil nodes is 5, there is a huge growth in the number of vulnerable nodes. In this configuration, there are 200 attack edges (double the number of honest nodes) and even though there are only 5 Sybil nodes, they will try to make 200 connections, thus there is an exceptional increase in the vulnerable nodes (blue curve).

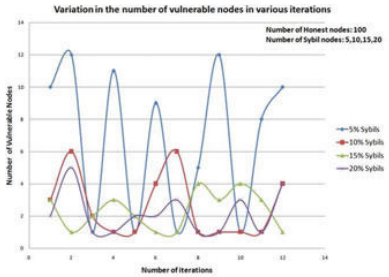
4.2 Clustering Coefficient

Clustering coefficient by varying the probability triad is determined in the graph is given in Fig. 7.

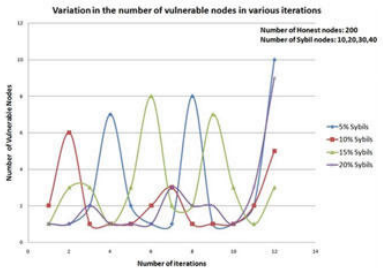
From the above graphs, we have observed that when the probability triad is varied in each iteration, gradually there is an increase in the clustering coefficient since this parameter is dependent on the value of triads. As a result, it can accelerate the rate of Sybil attack. If the maximum value of the clustering coefficient for a node is 1 then that node will have maximum degree (Fig. 7c).

4.3 Degree Distribution

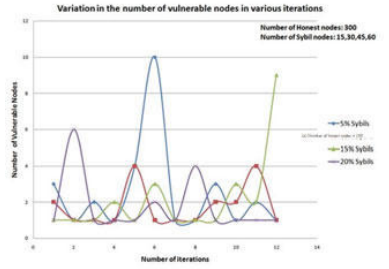
We plotted a graph for degree distribution as shown in Fig. 8. Since we use power graphs for the simulation of the two regions—honest and the benign regions—the degree distribution follows a power law distribution. Hence, we can observe that there is a long tail in the plotted graph.



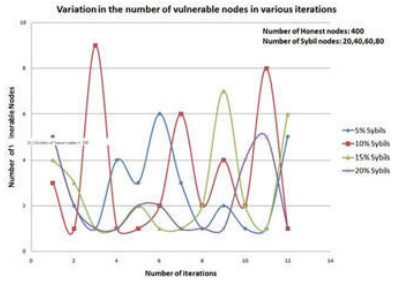
(a) Number of honest nodes = 100



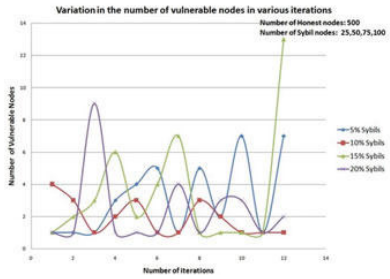
(b) Number of honest nodes = 200



(c) Number of honest nodes = 300



(d) Number of honest nodes = 400

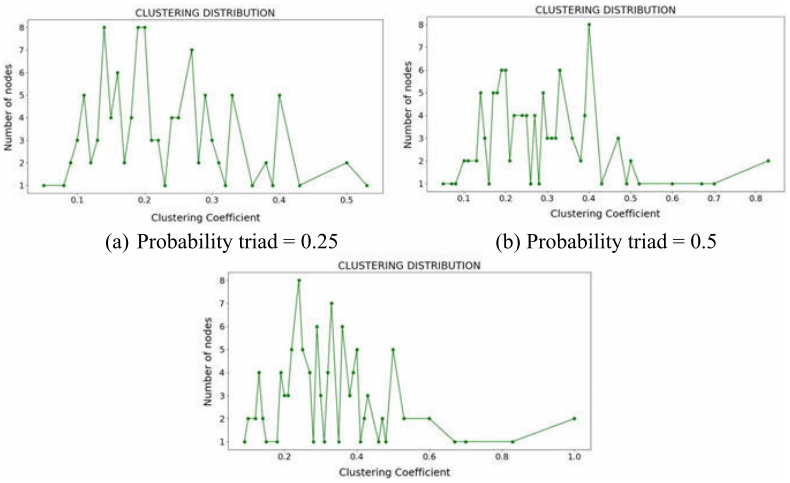


(e) Number of honest nodes = 500

Fig. 6 Variation in the number of vulnerable nodes in various iterations

5 Conclusion

Sybil attack is one of the major threatening problems in this era of social networks such that it questions the security and integrity of both the personal and public life of online users. In our work, we examined Sybil attacks in online social networks by applying SyPy Python package and thus we identified and analyzed the impacts of different parameters in the online social network that influences the Sybil attack.



(a) Probability triad = 0.25 (b) Probability triad = 0.5

(c) Probability triad = 0.75

Fig. 7 Clustering coefficient when probability triads is varied

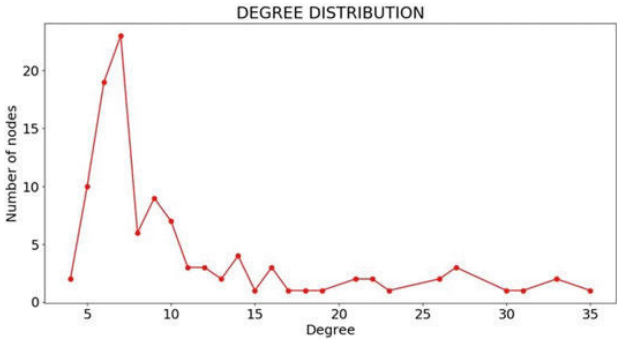


Fig. 8 Plot against the degree of the node and its frequency of occurrence

Our model can be applied to the real-world networks so as to detect users that are vulnerable to Sybil attack and avert them from these attacks.

References

1. Douceur, J.R., et al.: The Sybil attack. In: Druschel, P. (ed.) Peer-to-peer systems. Springer, Heidelberg, pp. 251–260 (2002)

2. Yu, H.: Sybil defenses via social networks: a tutorial and survey. ACM SIGACT News **42**(3), 80–101 (2011)
3. Viswanath, B., Post, A., Gummadi, K.P., Mislove, A.: An analysis of social network-based sybil defenses. In: Proceedings of the ACM SIGCOMM 2010 Conference on SIGCOMM, ser. SIGCOMM '10, pp. 363–374. ACM, New York (2010)
4. Boshmaf, Y., et al.; Graph-based sybil detection in social and information systems. In: Proceedings of ASONAM'13. IEEE (2013)
5. Boshmaf, Y.: A Quick Survey of Social Network-Based Sybil Defenses. University of British Columbia, Vancouver (to appear)
6. Viswanath, B., Mondal, M., Clement, A., Druschel, P., Gummadi, K.P., Mislove, A., Post, A.: Exploring the design space of social network based sybil defenses. In: 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS), pp 1–8, Jan 2012
7. Girvan, M., Newman, M.: Community structure in social and biological networks. Proc. Natl. Acad. Sci. **99**(12), 7821–7826 (2002)
8. Andersen, R., Chung, F., Lang, K.: Local graph partitioning using pagerank vectors. In: 47th Annual IEEE Symposium on Foundations of Computer Science, 2006. FOCS'06, pp. 475–486. IEEE (2006)
9. Mislove, A., Post, A., Druschel, P., Gummadi, K.P.: Ostra: leveraging trust to thwart unwanted communication. In: NSDI (2008)
10. Boshmaf, Y., et al.: Integro: leveraging victim prediction for robust fake account detection in OSNs. In: Proceedings of NDSS, pp. 8–11 (2015)
11. Jia, J., Wang, B., Gong, N.Z.: Random walk based fake account detection in online social networks. In: IEEE DSN (2017)
12. Alvisi, L., Clement, A., Epasto, A., Sapienza, U., Lattanzi, S., Panconesi, A.: SoK: the evolution of sybil defense via social networks. In: Proceedings of the IEEE Symposium on Security and Privacy (2013)
13. Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: Design and analysis of a social botnet. Comput. Netw. **57**(2), 556–578 (2013)
14. Wang, B., Gong, N.Z., Fu, H.: GANG: detecting fraudulent users in online social networks via guilt-by-association on directed graphs. In: IEEE ICDM (2017)
15. Pearl, J.: Probabilistic reasoning in intelligent systems: networks of plausible inference (1988)

Study on Data Transmission Using Li-Fi in Vehicle to Vehicle Anti-Collision System

Rosebell Paul, Neenu Sebastian, P. S. Yadukrishnan, and Parvathy Vinod

Abstract This paper examines the relevance of a fast approaching highly secure and fast data transmission technique using Li-Fi. It describes the upcoming technology Li-Fi and its applications as well as the developments made in it so far. It enlightens on the new era that will soon be used in almost all domains like health sector, school, bank and so on. An application framework design has been studied to analyze the role of Li-Fi in the process of communication.

Keywords Li-Fi · Light emitting diode (LED) · Wireless communication · IoT · V2V communication · Data transmission

1 Introduction

Light emitting diodes (LED) bulbs that are used in our household as light source are not only capable of lighting the surroundings but can also be used to transmit data. This idea forms the backbone of the new technology Li-Fi. Li-Fi stands for light fidelity and it uses LEDs intensity variation for transmission of data. It is very difficult or almost impossible for the human eyes to trace this variation as it happens too rapidly. We can say that Li-Fi is a light-based Wi-Fi technology. The Li-Fi revolution can possibly eliminate most of the problems of the existing wireless-fidelity infrastructure (Wi-Fi) in several core areas like medicine and health sector

R. Paul (✉) · N. Sebastian · P. S. Yadukrishnan · P. Vinod
Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, Kochi, India
e-mail: rosebell@scmsgroup.org

N. Sebastian
e-mail: neenusebastian@scmsgroup.org

P. S. Yadukrishnan
e-mail: yedhups@ieee.org

P. Vinod
e-mail: parvathyvinod@ieee.org

A. Pasumpon Pandian et al. (eds.), *Computer Networks, Big Data and IoT*, Lecture Notes on Data Engineering and Communications Technologies 66,
https://doi.org/10.1007/978-981-16-0965-7_41

since it evokes no electromagnetic reaction. The recent studies made in Li-Fi [1] reveal that it is going to be a part of the framework of 5G. It has been recognized by IEEE since the end of 2017, as an IEEE 802.11 working group has been formed for making the studies on standards for visual light communications. Wi-Fi has to abide to the country's particular regulations as it works with the spectrum allocation but Li-Fi does not.

Professor Harald Haasa German physicist, known as the founder of Li-Fi, introduced the term Li-Fi and he is the co-founder of PureLi-Fi which is a company based on light communication established by him in 2012 to work intensively on this new finding. He successfully illustrated a Li-Fi prototype at the TED Global conference in Edinburgh on 12 July 2011. He used a table lamp with an LED bulb to transmit a video that was then projected onto a screen. [2]. This idea pioneered by him gave a new direction to the researchers to explore more on the light waves [3].

In the next section, the basic principle of Li-Fi is explained followed by a briefing on a few applications of Li-Fi with several examples where it has already been implemented. In the Sect. 4, a comparative study is made with Wi-Fi. Section 5 describes the market growth of Li-Fi along with a study of converging Li-Fi with several emerging technologies. Section 6 is a prototype model framework illustrating the data transmission using Li-Fi in a vehicle to vehicle communication to avoid collision. Sections 7 and 8 show the analog and digital data transmission in our system. The results and inferences obtained from our experimental study are mentioned in Sect. 8. Finally, this paper is a journey through the developments made so far using Li-Fi and the authenticity of using Li-Fi for data transmission in analog and digital format is studied using the prototype model.

2 Principle of Li-Fi

Li-Fi can be termed as light-based Wi-Fi, i.e., instead of radio waves, it uses light to transmit data. In place of Wi-Fi modems, Li-Fi would use transceivers that have LED lamps that could brighten a room as well as transmit and receive information. It makes use of the visible portion of the electromagnetic spectrum which is hardly utilized.

LED bulbs or any light source can be used to transmit the data and the photodetector is used to detect the flash light emitted from the transmitter side. The data to be transmitted has to be encoded into a binary format which consists of a sequence of 1's and 0's. This binary stream of data is given as input to the LED light source and it will be transmitted when the LED glows. These flashes are then detected by the photosensors. The photosensors transfer the binary data for amplification, thereby strengthening the signal in order to decode the binary digits. Finally, the decoded data is transferred to the end device [4].

The block diagram of a Li-Fi transmitter and receiver system is depicted below.

Transmitter section consists of the Web server, modem and LED driver (Fig. 1).

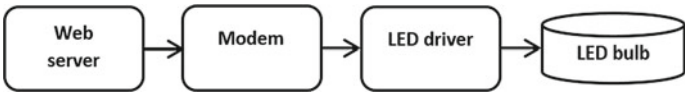


Fig. 1 Basic block diagram of the transmission section

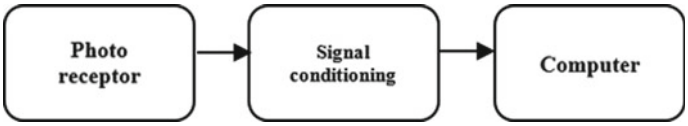


Fig. 2 Basic block diagram of the receiver section

Modem performs the necessary modulation to the incoming data, thereby making the data signals more suitable. As we change the intensity of the current send to the LED bulb, the brightness of the bulb changes which can then be converted into 1 s when illumination is maximum and 0 s when illumination is minimum. In this way the LED bulb is rapidly flickered, millions of time and is not visible to our naked eyes. In order to control this flickering properly, we make use of modulation. The three different types of modulation in Li-Fi are: single carrier modulation (SCK), multiple carrier modulation (MCK) and color modulation [2].

LED driver changes the driving current for this LED bulb according to the incoming streaming data to get the flickering. It plays the role in the conversion of digital signal to photonic signal.

Receiver section consists of the photoreceiver and is then given for signal conditioning before being transferred to the computer (Fig. 2).

Photoreceiver or the photodiode converts the optical signals received into electrical impulses. Signal conditioning mainly performs the necessary amplification and processing of the received signals before sending to the work devices. Thus, we can say that Li-Fi provides a one to one point of communication between any two devices in a highly secure manner. It has a speed much faster than the existing connection technologies. Though the term came into being in 2011, several studies and research are still being done to make it accepted all over the world. Since it makes use of the visible light spectrum, it can be used to pave way for communication at places where Internet access is denied like petrol pumps, operation theater, aircraft, etc. A study on the several applications developed using Li-Fi in several systems reveals that this technology will soon conquer the whole world. Li-Fi can protect the mankind from radio waves as the light spectrum used in Li-Fi does not penetrate through the body and is much safer when compared to the hazards caused by radio waves [5].

3 Applications of Li-Fi

3.1 Li-Fi in Medical Department

The radiation hazards caused to the human body can be drastically reduced if we make use of Li-Fi technology. The minute details of patients can be continuously monitored as long as there is a LED light in the room and the data transmission is done in such fast rate that emergency situation can be handled well. The main challenges in our hospitals are that the rooms require multiple access, and therefore the network becomes dense and heavy and complex cables are needed for the different equipment. The typical network architecture which consist of laying cables, installing routers, switches, etc., becomes difficult in hospitals. Schnell Li-Fi along with Huawei has come with the idea of all optical hospital in which they use Li-Fi and optic fiber as a better choice for hospital infrastructure. They called it green networks as Li-Fi technology uses passive light with no known health hazards. Similarly, Li-Fi is the best option in a room which has confidential information as it cannot be hacked. The photonics network will always be preferred in future for sensitive environment which consist of several medical devices as the Wi-Fi signals might interfere with the device signals at hospitals thereby affecting the readings. The various devices in the hospitals are connected to each other and may also require to transfer data to cloud for future analysis. As IoT enters the surgery room, Wi-Fi will become obsolete. The Li-Fi devices of Schnell were proven to be compatible with the Huawei and so they just had to plug and play making it easy to assemble and reconfigure. Thus, Li-Fi provides wireless connectivity for telemedicine, lifesaving applications, hospital security systems and vital body sensors. Similarly, Li-Fi indoor positioning system can optimize the navigation within the hospitals [6].

3.2 Li-Fi in Aircraft

For the first time in world, Air France A321 tested Li-Fi Technology during a flight in a 12-seater specially designed aircraft in which the travelers could play video games. By working on it for a short time span of a little of 6 months they built the system and successfully used Li-Fi describing it to be a much simpler technology than the traditional equipment they used and hosted the Air France Trackmania Cup in October 2019. They used fiber optic cables to transmit the light-based Internet access. They installed a baggage compartment which acts as the server that was designated to transmit the data notably the video games. They had installed a dedicated headrest for the screen and a dongle for transmitting Li-Fi communications. A detector was installed for optical transmission. Thus, Li-Fi enabled 10 gamers to play together and it is several times faster than Wi-Fi, thereby provided a more viable experience.

The ability to safely access the Internet at 30,000 ft is becoming commonplace nowadays. However, as passengers place greater demands on the in-flight Internet

bandwidth, the connected experience could become less of a benefit to the experience and more of a frustration, because airplane mode blocks your connection to cellular networks and it is not possible to communicate or make calls using phone calls. The airplane mode will turn off the Wi-Fi connection and thus will abrupt all the services that requires Internet connectivity.

Li-Fi solves a 'congestion' issue. In the data-driven world that we live in, we are running out of radio spectrum. This is a problem in crowded places like airports and aircraft interiors as it means that the current available bandwidth does not support the hundreds of people wishing to use data-intensive applications and the Internet in the same place at the same time. Li-Fi solves this issue by using 1000 times the bandwidth compared with the entire radio frequency spectrum. This is additional free, unregulated bandwidth in the visible light spectrum.

Li-Fi paves the way for local area networks to be established, which means that passengers can make calls, use the Internet and access in-flight entertainment systems more easily.

In a world fast being dominated by big data, safeguarding information is paramount. In the cabin, although Li-Fi signals can leak through windows, the technology offers greater protection to passengers than a Wi-Fi connection. But the biggest gains will be experienced by OEMs. Their manufacturing halls often have lots of LED lighting and few windows, which will enhance data security in their facilities.

3.3 Underwater Communication System Using Li-Fi

The underwater communication system is a research area of great demand as the limitations in bandwidth, energy consumption of the devices used and distance pose a big challenge. The underwater communication system based on Li-Fi technology provides protection against ship collisions on the sea. Most remotely operated underwater vehicles (ROVs) are controlled by dedicated wired connections. Since light can travel through water, Li-Fi based communications could offer much greater mobility. An underwater communication system utilizing visible light communication (VLC) technology will be ideal for military and scuba divers operating under vessels, allowing communication within the light spectrum to a certain radius via an audio system built into their diving suits. This project focuses on the safety of the sea in which the headlights, which consist of LEDs acting as transmitters, communicate with photosensors acting as receivers. White LEDs used in the head and tail lights can effectively be used for short-range communication with the photodetectors. The application is cost effective as LEDs are cheap and simple algorithms are proposed for signal generation and transmission.

A study on the usage of Li-Fi for underwater communication by observing the propagation of visible light which is affected by inherent optical properties absorption and scattering is made in. It describes the bio-optical model which concentrates on the chlorophyll approach of propagation of light in seawater [7].

Recently, SaNoor's Laser Li-Fi Solutions used laser-based rays underwater for data transmission and to link several devices and allow Internet of underwater things. They claim that this technology enabled them to allow transmission at giga bytes per second. This system removed all the hassles created in the several existing underwater data transmission systems which consists of lot many of wires as well as and has limited operational range. The signal was sent from seafloor passing through sea and air in spite of the constant motions of the sea waves as well as the foams and bubbles. They found this solution useful for many applications like underwater pipe leak monitoring, underwater environment monitoring, offshore wind fan, etc.

3.4 Li-Fi in Office Rooms

PureLi-Fi came up with a fully networked Li-Fi system by the end of 2017. In the Li-Fi-enabled boardroom, they equipped six lights and it was more than enough for any kind of uninterrupted streaming services. They had come up with a dongle in 2016 which can be connected via universal serial bus to the laptops or other devices on which we need the data transfer and Internet connectivity. This dongle consists of a photodiode and the Infrared transmitter which is used to transfer data back to the LED source. PureLi-Fi had then revealed their future plan of making of semiconductor technology to neutralize this usage of dongle and make Li-Fi core-integrated.

BeamCastor is a Li-Fi-based local area network which was developed by a Russian company Stins Coman in 2014. In this, they made use of a router which was capable of transmitting signal using a light beam that had a coverage of approximately 7–8 m. It was successfully transmitted to eight devices at same time placed at different positions in the office and achieved a four times faster rate than Wi-Fi. The transmission model has to be installed on the ceiling and the receiver model is configured on the work devices. The key highlights of this system were the mobility and the ease of configuration and it could be easily disassembled.

3.5 Li-Fi in V2V and V2I Communication

Vehicle to vehicle communication (V2V) has an underlying wireless protocol called dedicated short-range communications (DSRC). A lost cost V2V communication system is developed DSRC and global positioning system (GPS). The vehicle controlling information such as transmission rate, brake status, speed, acceleration, global positioning and path history are taken into consideration to prevent crashes. With the help of these information if a vehicle in front puts a sudden brake suitable transmission of warning signal can be sent. Similarly, if a vehicle in front makes a slow movement and the vehicle you are driving is moving at pace faster, it might cause a

collision. V2V communication helps to pass the alert on time using the wireless communication. Li-Fi technology can be clubbed suitable in this system as it is having high speed transmission rate which will help in this time critical situations to prevent accidents [8].

In case of traffic system, Li-Fi can be used to enable the vehicle to infrastructure communication (V2I) as the LED in the traffic lights can act as the medium to pass signal to the first car in the lane. This car can then transmit this information to the one behind it. The one to one point communication technology principle of Li-Fi helps to ensure secure communications without congestion. The usage of Li-Fi in smart traffic net which is soon going to be the upcoming transportation system has been described in [9].

4 A Comparative Study Between Li-Fi and Wi-Fi

4.1 Wi-Fi Technology

Wi-Fi is an existing wireless networking technology which was invented by NCR corporation in 1991 and is widely in use. By using this technology, we can exchange the information between two or more devices. The radio waves act as the medium thereby making the Wi-Fi networking possible. Wi-Fi uses routers and radio frequency and the radio signals are transmitted from antennas and routers. These signals are picked up by Wi-Fi receivers, such as computers and cell phones that are ready with Wi-Fi cards. Wi-Fi is used for Internet browsing with the help of Wi-Fi kiosks or Wi-Fi hotspots. Wi-Fi data transfer speed ranges from 150 to 2 Gbps. It has a coverage area of up to 32 m Wi-Fi radiations that can harm human health. It is not suitable for airlines and undersea communications.

4.2 Comparison with Li-Fi System

(a) System Requirements: Li-Fi only needs lamp driver, LED bulb and photodetector which are not at all expensive. Wi-Fi requires routers to be installed and subscriber devices are referred as stations.
(b) Capacity: The visible light spectrum is several thousand times larger than the spectrum of radio waves. For visible light, the frequency ranges from 400 to 700 THz, but for radio waves, the range is from 3 kHz to 300 GHz. Thus, Li-Fi signals which are based on visible light spectrum will definitely have a larger capacity.
(c) Efficiency: LED lights consume less energy and are highly efficient. Li-Fi can successfully work in a high dense environment, whereas Wi-Fi can flawlessly work in less dense environment due to interference related issues.

(d) Availability: Light sources are present in every nook and corner of the world. Hence, the availability is not an issue. The billions of light bulbs worldwide need only be replaced by LEDs.

(e) Interruption: Light of course does not cross the walls and thus data transmission using light waves is more secure than Wi-Fi where the radio waves can penetrate across the walls. Thus, it is not easy to intercept the data transmitted via light beam, but hackers can eavesdrop the data transmission using Wi-Fi. On observing the electromagnetic spectrum, the bandwidth of the radio waves is up to 300 Ghz. The bandwidth of the visible spectrum alone is up to 300 Thz which approximately thousand times more compared to the bandwidth of the radio waves. Thus, apart from attaining higher speed, there will not be any electromagnetic interference.

(f) Data Transfer Speed: 4G LT and LTE advance have a maximum of 1 Gbps for stationary users and 100 mbps for mobile users which are theoretical figures and the actual speed might be lesser than these. The average 4G LTE speed provided by countries with highest Internet usage is 40–50 Mbps. Researchers have found up to 10 Gbps in Li-Fi prototype models. This speed can be increased more by using array of LED source or by using the multiple color RGB LED's where each of it can transfer at a speed of 10Gbps. In such a manner up to 100Gbps, when the whole visible spectrum can be used. Wi-Fi standards IEEE 802.11.ac have a maximum 1.3 Gbps transfer speed which comes under 5 GHz band and IEEE 802.11.ad provide a maximum speed of 7Gbps as defined theoretically. Though these speeds are enough to meet our daily need now, as we step into the era of Internet of things, these might not be enough and there comes the urge of maybe 100 Gbps where Li-Fi comes into effect. Thus, Li-Fi is ten times better than the current Wi-Fi on the basis of speed [10].

(g) Coverage: Li-Fi coverage depends on the intensity of the light but expected coverage is 10 m. Wi-Fi provides about 32 m (WLAN 802.11b/11 g) and it will vary based on the transmit power and antenna type.

(h) Technology: Li-Fi present Infrared Data Association (IrDA) compliant devices and Wi-Fi presents WLAN 802.11a/b/g/n/ac/ad standard compliant devices [11].

Specification	Li-Fi	Wi-Fi
System requirement	LED bulb, photodetector	Router, subscriber devices
Capacity	400–700 THz	3 KHz–300 GHz
Efficiency	Consume less energy and highly efficient	Affected by inference and less efficient
Availability	Light sources and widely available	Need special requirements
Data transfer rate	Very high (~1Gbps)	Low (100 Mbps–1 Gbps)
Cost and power consumption	Low	High

(continued)

(continued)

Specification	Li-Fi	Wi-Fi
Coverage	~10 m (depending upon the intensity of light)	~32 m (depending upon the transmitting power and antennae type)
Technology	Infrared data association (IrDA) compliant devices	WLAN standard compliant devices

5 Li-Fi in the Industry and Convergence of Li-Fi with Emerging Technologies

There are many companies that have started to bring the Li-Fi-based products into the markets.

PureLi-Fi, co-founded by Professor Harald Haas, provides kits to support the evaluation of high speed Li-Fi components, light antenna technology for integration into the mobile devices and the systems that allows to deploy Li-Fi.

Oledcomm is providing Li-Fi network interface devices. And they are concentrating on improving the design of Li-Fi router solutions for LED-based systems.

LightBee is working on automotive control access and car2car communications modules.

Velmenni, Firefly, Lucibel, LightBee, LVX System, Signify, Vlncomm, LIFX, Luciom are a few of them which are all concentrating on Li-Fi technology. According to the survey made by marketresearchfuture.com, Li-Fi market is expected to grow at approx. USD 51 Billion by 2023, at 70% of CAGR between 2017 and 2023. Because of the revolution in the technical world where all the devices are getting connected high speed of data transmission is going to be a matter of prime concern and foreseeing this many companies like General Electric and Philips are investing into Li-Fi market.

5.1 Li-Fi and IoT

Internet of things is a system of interrelated computing devices which can exchange information and transmit data without human interaction. IoT devices comprises of several sensors, actuators, connectivity/communication electronics and software to capture, filter and exchange data about themselves, their state and their environment. However, this widespread development in IoT which interconnects larger scale of heterogeneous devices creates a big challenge so as to how to safeguard the hardware and the networks in the IoT system and transfer data without interferences and delay [12]. Thus, integrating the Li-Fi concept with IoT provides solutions to a wider

variety of problems in different domains. Unipolar orthogonal frequency division multiplexing (U-OFDM) which is used in Li-Fi technology gives high speed data transmission along with room illumination. As a result, enough bandwidth is obtained to accommodate large number of IoT devices [13]. Massive multiple input multiple output (MIMO) which consists of several antennas at the transmitter and receiver based on visible light spectrum will have higher bandwidth [14].

5.2 Li-Fi and Cloud

Cloud acts a centralized storage and it allows to store, manage and process data over the Internet using large group of servers based on virtualization technology. The data is stored and retrieved in a data center, instead of locally on the user device. As IoT-enabled environment requires large amount of data to be stored and processed frequently, cloud makes it possible to enable access of the same data and applications from any part of the world. The increasing demand of wireless communication has posed a problem of acquiring real-time data without latency delay and bandwidth bottleneck problems from cloud. In the existing IoT network, especially in highly dense environment, the available radio spectrum becomes insufficient. Li-Fi due to its high speed and greater bandwidth can be a stand in such a scenario. The challenges of the existing cloud IoT paradigm and a Li-Fi-based hybrid cloud framework study are described in [15]. In their study, a layered architecture comprising of infrastructure layer or the physical layer, local or private cloud layer and global or public cloud layer is proposed. The communication between the local cloud and the IoT devices in the physical is established using Li-Fi enabled access point which acts as a forwarding device. The IoT devices will be embedded with LED and photodiode which will make the light communication possible [12].

5.3 Li-Fi and Real-Time Analytics

Time critical applications such as tracking and navigation are mainly based on real-time analytics. The large amount of data gathered is analyzed by applying logic and mathematical concepts to make conclusions, decisions and future predictions. The current business world which concentrates on making all the services much easier for customers keeps a constant watch on the data which can be the customer behavior pattern and gives suggestion for the next activity based on the analysis. This can be applied in the area of online shopping, medical sector, traffic system and so on. The Li-Fi-based companies have already started working with the real-time data analytics using the data which gets stored on their cloud using indoor positioning system (IPS). IPS is a system similar to global positioning system (GPS) but it is within the indoor environments where the satellite technologies are less efficient.

There are different technologies for IPS like acoustic systems, proximity based, infrared systems, Bluetooth based and so on. GeoLi-Fi is a Li-Fi-based geolocation platform by Li-Fi supporting companies like Basic6 and Oledcomm for indoor environments. Light fidelity access point installed in a dense network will gather accurate location information and create a map. The system comprises of Li-Fi LEDs that stream information as unique identifiers, LED Li-Fi modulator which transforms LED lights into a very simple Li-Fi antenna, Li-Fi-enabled tablets utilizing software communicate to consumers, centralized managerial interface and tools to perform the analytics, planning, forecasting and management. Each of the light source has a unique identifier and a mapping is defined of where all these lights are located and a unique identifier for those positions [16]. The tablets which are customized with the photodiode, and therefore whenever the tablet is under the Li-Fi enabled light its location is accurately identified. Instead of customized tablets, it is also possible to make use of Li-Fi-enabled dongle which can be easily plugged into our smartphones.

This system can be used in big supermarkets and the customer shopping pattern which is tracked using IPS is sent to cloud, real-time analytics can be applied, and thus the future shopping pattern can be predicted accurately. It can also make the shopping process much easier by giving information regarding the necessary item's location in the store and any additional information regarding it. This Li-Fi-based IPS can also be installed in emergency places like hospitals so that optimized navigation can be made without any delay [6].

6 Prototype Description

In this prototype, light is used as a medium of transmission. With the advent of Internet of vehicles, the entire traffic is going to be automated soon. Hence, using the headlights of the vehicles, an automated brake system can be implemented with Li-Fi support [2]. Earlier spread spectrum mechanisms were used in order to meet the needs of communication between vehicles. The military vehicle services are maintained and scrutinized based on the spread spectrum methodology.

A major drawback of the traditional system is that it requires the complete attention of the driver to control the speed and occurrence of a collision. But according to the proposed system in [2], the alert signal send to the vehicle as demonstrated with the help of light signals. Here, automation can be achieved as the distance between the vehicles if reduces below a specific limit and the controller reacts and hence avoid the accident. Basically, the light rays emitted by the car at the front through the brake light/stop light will be received by the car behind through a receiver at the front bumper which triggers the car according to the situation. As the emission is purely based on light rays, there is no chance of environmental issues or scattering of important signals.

6.1 Hardware Requirements

(a) Arduino UNO: The Arduino Uno is a microcontroller board based on the Microchip ATmega328P microcontroller and it is programmed with the help of an open-source Arduino software. This software acts as an integrated development environment (IDE) which will help to perform coding on the computer side and upload it to the physical board. Thus, we can say that Arduino UNO has hardware and software parts. The hardware section of the board comprises of digital and analog input/output (I/O) pins that may be interfaced to other circuits. This Arduino UNO is enough for the data transfer from one device to another.
(b) LED: Li-Fi bulbs are outfitted with a chip that modulates the light imperceptibly for optical data transmission. Light emitting diodes (LEDs) are used in Li-Fi as visible light transmitters. Li-Fi data is transmitted by the LED bulbs and received by photodiodes. The LED is connected to one of the digital pins. The LED blinks according to the binary logic sent from the processing software.
(c) LDR: An LDR is a component that has a (variable) resistance that changes with the light intensity that falls upon it. It is a passive component, which uses the concept of photoconductivity and has a resistor whose resistance value decreases when the intensity of light decreases. This optoelectronic device is mostly used in light varying sensor circuits. The light from the LED is identified by using LDR and the data is transmitted to the Arduino.
(d) Solar Panel 5v: In our system, it acts as a data receiver of analog digitals. Here, we have used 5v solar panel. In our system, solar panel acts as a data receiver of analog signals and not a power source. The LED light source combined with a solar panel can form a transmitter-receiver system. LED transmits encoded information which is received by the solar cell and made available where the information is required.
(e) Ultrasonic Sensor: An ultrasonic sensor is an electronic device that measures the distance of a target object by emitting ultrasonic sound waves and converts the reflected sound into a signal. In our system, the ultrasonic sensor is fixed in front of our vehicle and it measures the distance between the car and obstacle in front and gives an alerting signal if the distance is beyond a certain limit.
(f) Speaker and audio amplifier
(g) LCD display and batteries.

6.2 Software Requirements

(a) Arduino programming language: Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or integrated development environment (IDE) that runs on your computer, used to write and upload computer code to the physical board. The

IDE supports C and C++ and includes libraries for various hardware components, such as LEDs and switches. The program which is also known as sketch is uploaded to the Arduino board via a USB cable. Here, it can be run and will remain in memory until it is replaced.

(b) Python IDLE: Python IDLE is an integrated development environment (IDE) for Python. The Python installer for Windows contains the IDLE module by default. IDLE can be used to execute a single statement just like Python shell and also to create, modify, and execute Python scripts.

(c) Tinkercad: Tinkercad is a free, online 3D modeling program that runs in a Web browser, known for its simplicity and ease of use. We have used it to stimulate circuits and to generate Arduino codes.

7 System Design

The system uses the ultrasonic sensor which reads the distance to the obstacle in front of the vehicle where the sensor is fixed. The distance is then sent to the Arduino UNO. Basically, the light rays emitted by the car at the front through the brake light/stop light will be received by the car behind through a receiver at the front bumper which triggers the brake according to the situation. As the emission is purely based on light rays, there is no chance of environmental issues or scattering of important signals.

The prototype makes a study on digital and analog data transmission. For analog data transmission, we made use of audio source, LED, solar panel and audio amplifier.

7.1 Analog Data Transmission

See Fig. 3.

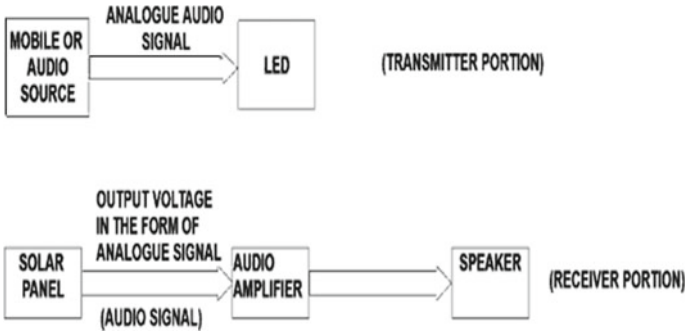


Fig. 3 Block diagrams of analog data transmission

7.2 Schematic Diagram for Analog Data

(a) Transmitter Section:

Depending upon the change in the music which is the analog signal the LED glows and its light intensity varies according to the fluctuations in the analog signal (Fig. 4).

(b) Receiver Section

At the receiver side, solar panel is used for light detection from the transmitter side and it then given to an audio amplifier followed by the speaker (Fig. 5).

8 Digital Data Transmission

The light signals emitted from the vehicle at the front will be received by the car behind via an LDR. Light-dependent resistors are very sensitive to light. When the required signal reaches the LDR, the input is also obtained. Ultimately when the distance between the vehicle or vehicle and the object is less than or equal to predefined limit known as safe distance, and the vehicle itself will apply brakes to

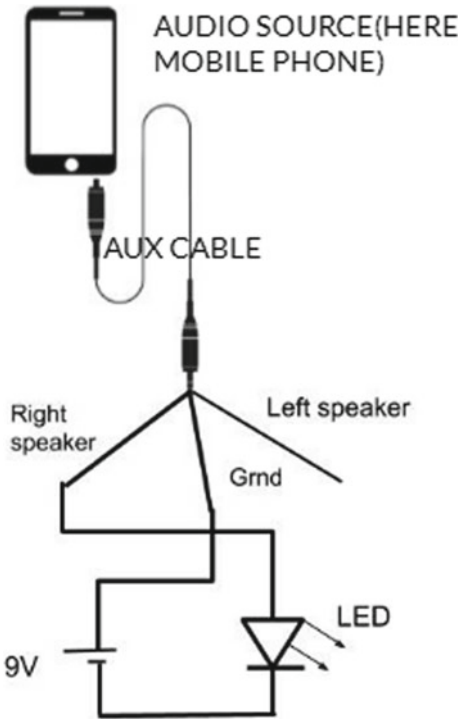


Fig. 4 Block diagram of transmitter section

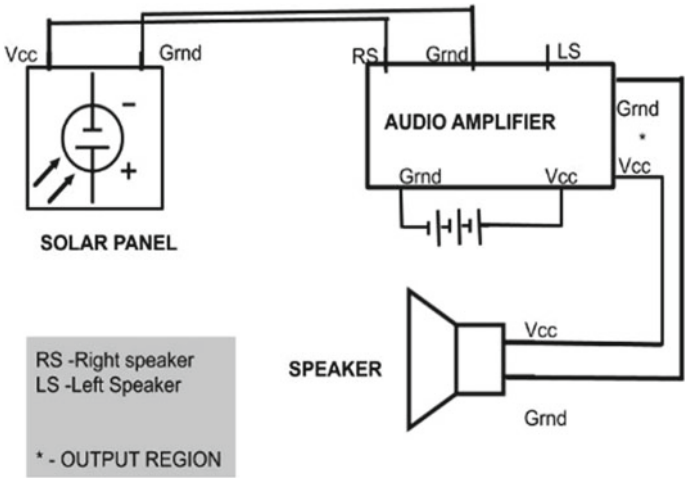


Fig. 5 Block diagram of receiver section in analog data transmission

avoid the accident. If the distance between the vehicle are more than the defined safe distance, then the system will give a warning and emergency notification to the driver as a safety measure. The distance between the car and obstacle is measured by the ultrasonic sensor and then passed on to the Arduino UNO. Then, if it is less than the limit, then it is passed on to the LED and then the LED blinks accordingly.

8.1 Transmitter Section

The value measured using ultrasonic sensor is stored into a variable, say 'time'. We then take the half of it and store it in a variable 't'. This value is used to compute the distance which is calculated as 340/t, as 340 m/s is the speed of the sound in air. The safe distance between car and the object is taken as 15 or above for our study. Here, a checking is done again to find if it is less than or equal to 5 and if so the LED glows for a time duration of 25 ms indicating brake should be applied otherwise the LED will glow for a time duration of 20 ms which is a warning sign. This is how the transmitter gets activated and starts sending data as Li-Fi signals and is depicted in the flowchart of the transmitter section (Fig. 6).

Fig. 6 Block diagram of transmitter section in digital data transmission

8.2 Receiver Section

The LDR records data from the LED blink in 0 s and 1 s. It is then passed on to Arduino UNO and the alert or the warning message is sent. Here, instead of buzzer system, we used an LCD display. The value read from LDR is stored in a variable 'd'. In the next 20 ms, LDR value taken is stored to the variable val2. A string variable duration is concatenated with this val2. If val2 value is 1, then we perform a checking of whether duration is '0001' and if so it displays a warning in the LCD Display else if the duration is '00001' it causes the braking system to be enabled. The flowchart for the receiver section depicts this process (Figs. 7, 8 and 9).

The digital data transmission is represented as depicted in the flowchart (Figs. 10 and 11).

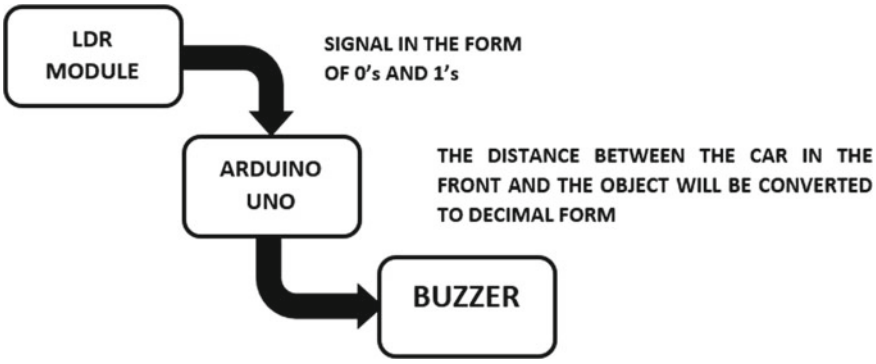


Fig. 7 Block diagram of receiver section in digital data transmission

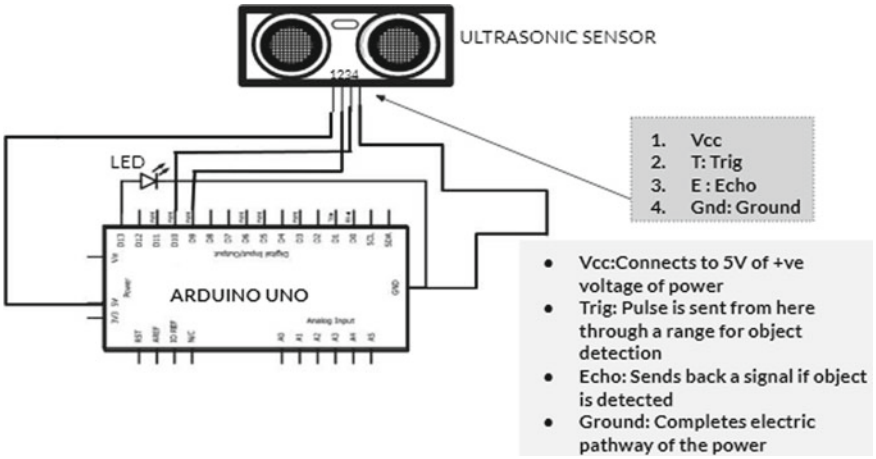


Fig. 8 Schematic diagram of digital data transmission section

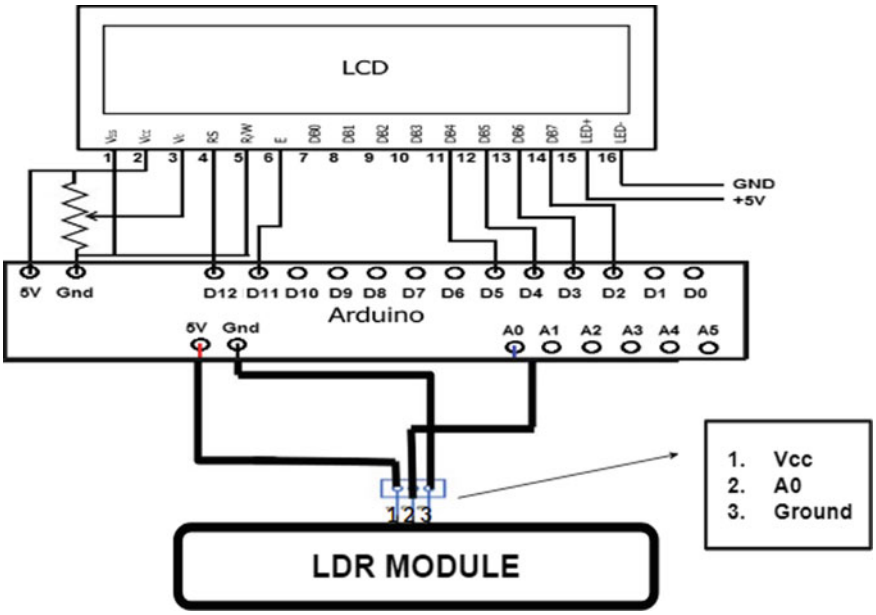


Fig. 9 Schematic diagram of digital data receiver section

9 Results

In the system showing analog data transmission, we inferred that the speaker produces sound only when it is exposed to a light which is having Li-Fi signals. In the digital data transmission system, the audio signal from the mobile phone using AUX cable and was given to the Arduino. And this is the output waveform which we got from the Arduino. Now, it is clear that Li-Fi is an ideal point to point communication medium among two vehicles.

The plot that the signals have a voltage level variation depending upon the light signals. Similarly, the pattern was observed by varying the sensitivity of the LDR module to ensure the promptness of Li-Fi. We have voltage measured in the *y*-axis and the time taken in the *x*-axis.

The first plot shows output from solar panel when there are no variations (Figs. 12, 13 and 14).

10 Limitations and Challenges

1. Difficulty in calibrating the Li-Fi receiver in presence of ambient light.
2. The distance between the Li-Fi transmitter and receiver affects the visible light communication (VLC) technology.

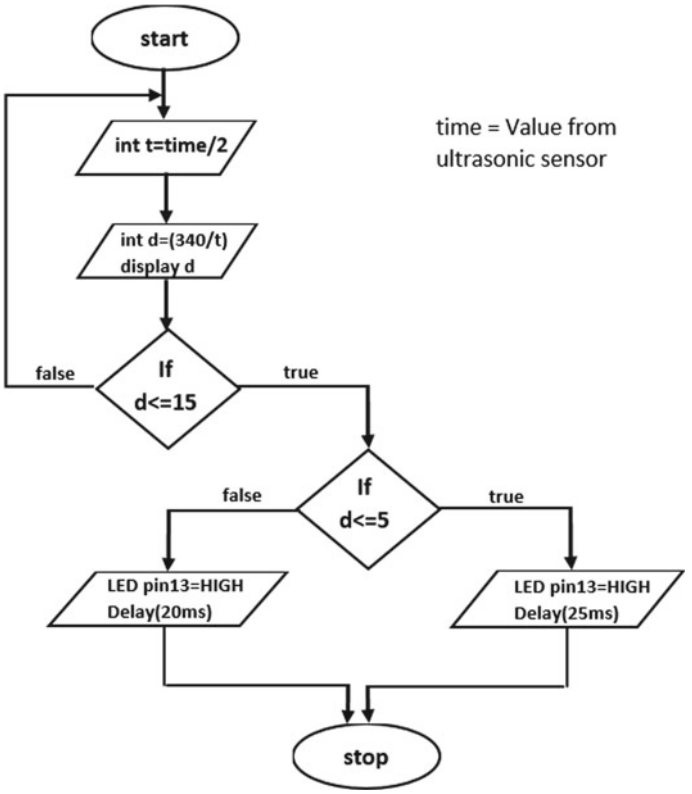


Fig. 10 Flowchart of transmission section

3. In some cases, the shorter range of Li-Fi communication, Li-Fi put forwards security features.
4. We can use laser for long-range Li-Fi communication/data transfer, but in this case, the components of the setup should be in a fixed position.
5. Refraction cases Li-Fi signal loss
6. The modulation in Li-Fi is a challenge when the light illumination is low.
7. Li-Fi should need line of sight for effective data transmission. Small difference leads to interruption in the transmission.

11 Conclusion and Future Works

Li-Fi era is not too far and there are many companies who have started marketing products based on Li-Fi technologies. There are many countries where Wi-Fi usage is narrowed due to its harmful effects especially for children and health sectors. Li-Fi will predominantly gain wide spread popularity in those places because of its secure

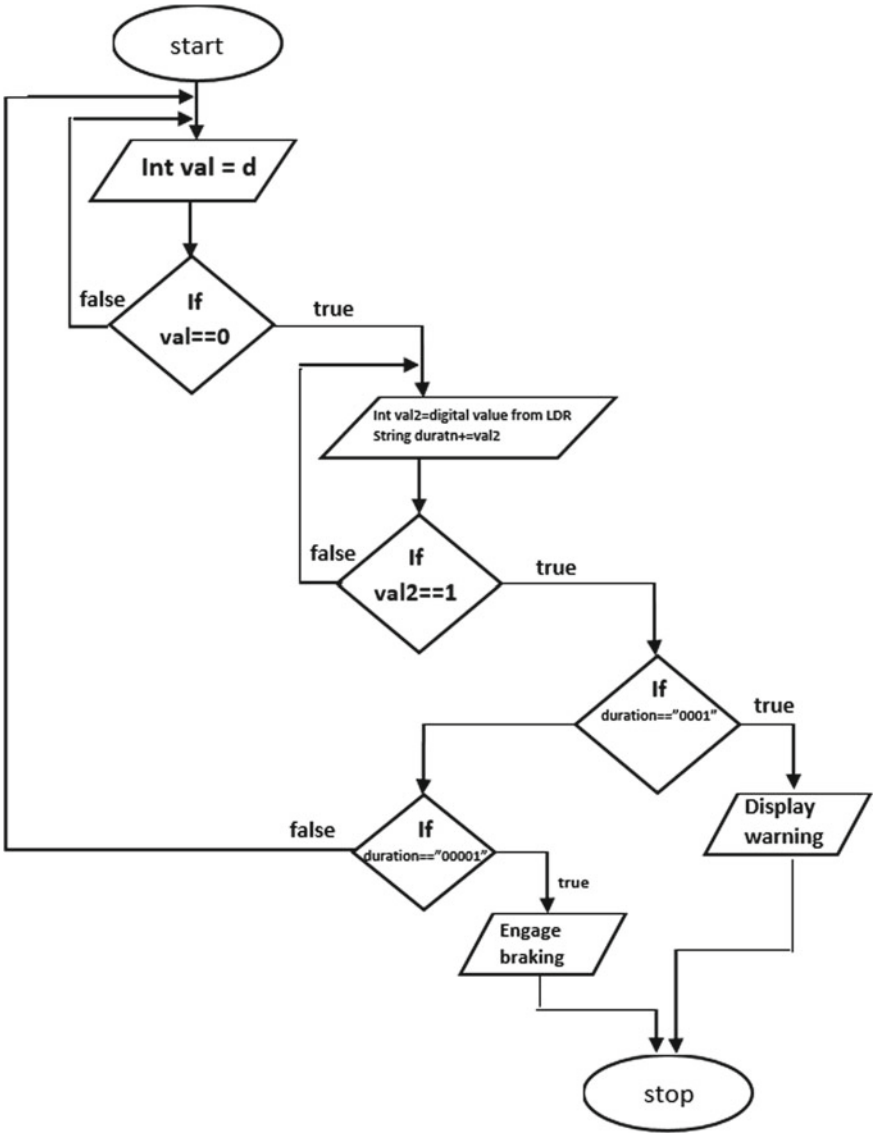


Fig. 11 Flowchart of receiver section

and environment-friendly nature. It will gradually conquer the whole world and as predicted by the researchers working on it. As the wave made by photon produced by a light emitting diode has no power to penetrate through the skin it will soon be a safer substitute for the electromagnetic waves in the field of communication which can penetrate through even walls. In hospitals, where real-time health monitoring is

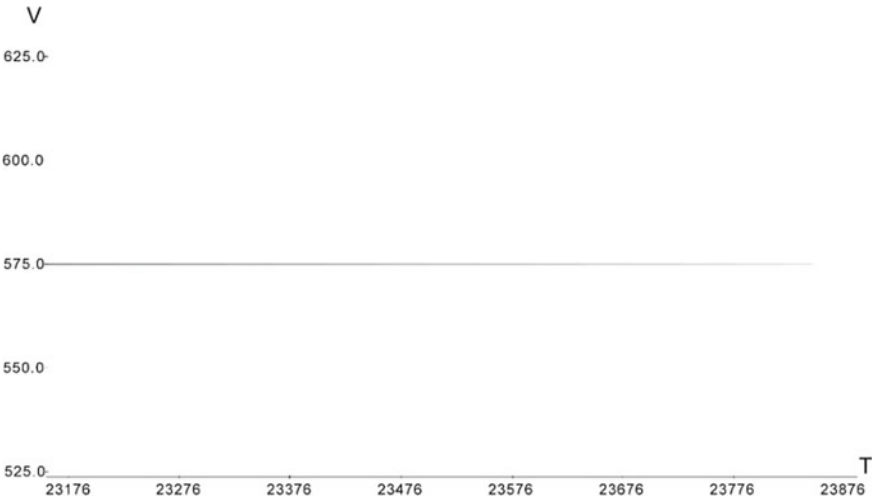


Fig. 12 Graph showing the output from solar panel under a tube light (i.e., when there is no variation)

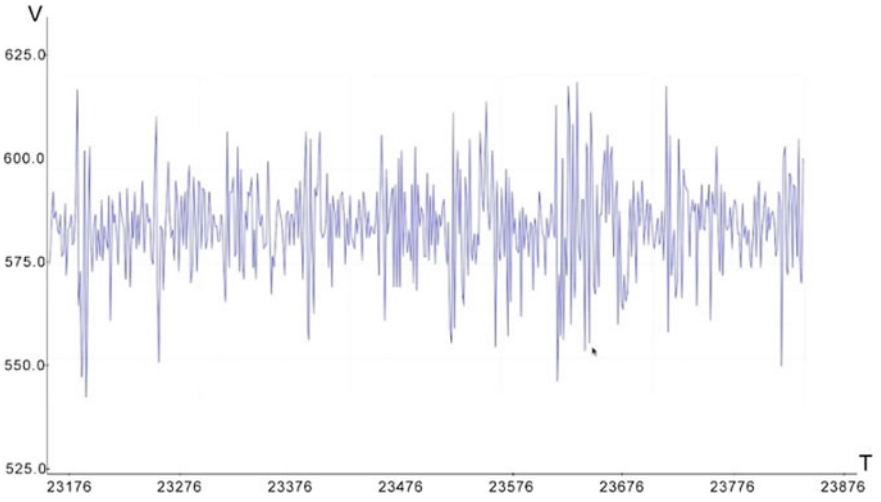


Fig. 13 Graph showing the output from solar panel under a light integrated with audio signal

extremely time critical, Li-Fi can be used as it provides high speed. Li-Fi as elaborated in the applications can play predominant role in aircraft, underwater systems, vehicle to vehicle communications and other infrastructures. Even our street lamps can provide us with high speed Internet with the Li-Fi technology.

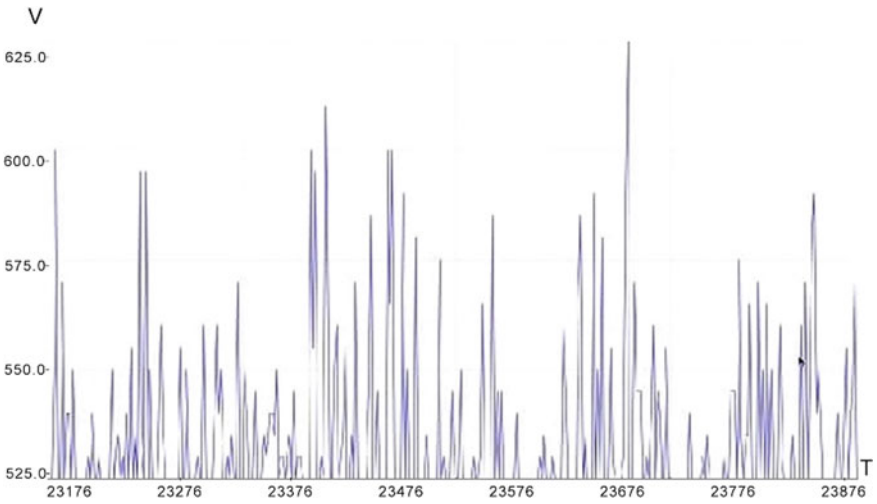


Fig. 14 Graph showing the output from Arduino when audio signal from a mobile phone using AUX cable

References

1. Ayyash M, Elgala H, Khreishah A, Jungnickel V, Little T, Shao S, Rahaim M, Schulz D, Hilt J, Freund R (2016) Coexistence of Wi-Fi and Li-Fi towards 5G: concepts, opportunities, and challenges. IEEE Commun Mag 54. https://doi.org/10.1109/mcom.2016.7402263
2. George R, Vaidyanathan S, Rajput A, Kaliyaperumal Da (2019) Li-Fi for vehicle to vehicle communication—a review. Procedia Comput Sci 165:25–31. https://doi.org/10.1016/j.procs.2020.01.066
3. Matheus LEM, Vieira AB, Vieira LFM, Vieira MAM, Gnawali O (2019) Visible light communication: concepts, applications and challenges. IEEE Commun Surv Tutorials 21(4):3204–3237, Fourthquarter. https://doi.org/10.1109/comst.2019.2913348
4. Ramadhani E, Mahardika GP (2018) The technology of Li-Fi: a brief introduction. In: IOP conference series: materials science and engineering 325(2018):012013. https://doi.org/10.1088/1757-899x/325/1/012013
5. Lokesh S, Priya N, Divyakanni K, Karthika S (2017) A Li-Fi based data transmission for anti-collision system. Int J Smart Sens Intell Syst 212–224. https://doi.org/10.21307/ijssis-2017-247
6. Yu HK, Kim JG (2019) Smart navigation with AI engine for Li-Fi based medical indoor environment. In: 2019 International conference on artificial intelligence in information and communication (ICAIIC), Okinawa, Japan, 2019, pp 195–199. https://doi.org/10.1109/icaiic.2019.8669041
7. Balaji K, Murugan SS (2019) Implementing IoT in underwater communication using Li-Fi. Int J Recent Technol Eng (IJRTE) 8(2S4). ISSN: 2277-3878
8. Hernandez-Oregon G, Rivero-Angeles ME, Chimal-Eguía JC, Campos-Fentanes A, Jimenez-Gallardo JG, Estevez-Alva UO, Juarez-Gonzalez O, Rosas-Calderon PO, Sandoval-Reyes S, Menchaca-Mendez R (2019) Performance analysis of V2V and V2I Li-Fi communication systems in traffic lights. Wirel Commun Mobile Comput 2019:12, Article ID 4279683. https://doi.org/10.1155/2019/4279683
9. Panhwar M, Khuhro SA, Mazhar T, Zhongliang Deng (2020) Li-Net: towards a smart Li-Fi vehicle network. Indian J Sci Technol 13:1–9. https://doi.org/10.17485/ijst/v13i18.210

10. Leba M, Riurean S, Lonica A (2017) Li-Fi—the path to a new way of communication. In: 2017 12th Iberian conference on information systems and technologies (CISTI), Lisbon, 2017, pp 1–6. https://doi.org/10.23919/cisti.2017.7975997
11. Kuppusamy P, Muthuraj S, Gopinath S (2016) Survey and challenges of Li-Fi with comparison of Wi-Fi. In: 2016 International conference on wireless communications, signal processing and networking (WiSPNET), Chennai, 2016, pp 896–899. https://doi.org/10.1109/wispnet.2016.7566262
12. Smys S, Basar A, Wang H (2020) Artificial neural network based power management for smart street lighting systems. J Artif Intell 2(01):42–52
13. Pottoo SN, Wani T, Dar A, Mir A (2018) IoT enabled by Li-Fi technology
14. Al-Ahmadi S, Maraqa O, Uysal M, Sait SM (2018) Multi-user visible light communications: state-of-the-art and future directions. IEEE Access 6:70555–70571. https://doi.org/10.1109/ACCESS.2018.2879885
15. Sharma P, Ryu J, Park K, Park J, Park J (2018) Li-Fi based on security cloud framework for future IT environment. Human-centric Comput Inf Sci 8. https://doi.org/10.1186/s13673-018-0146-5
16. Sungheetha A, Sharma R (2020) Cost effective energy-saving system in parking spots. J Electron 2(01):18–29

Excavation of Time sliced and Cost based KDD for the lead generation and promotion on B2C/B2B Sales

Publisher: IEEE

Jency Rena NM

Department Of Computer Science and Engineering, SCMS School Of Engineering and Technology

All Authors

since they are dealing only with the number of times an item appears in the database. In business environments like retail shops or online markets, identifying the profit-generating items is more important than finding the items which are sold many times. The high utility item set mining with the time cube concept helps us to find the relevant, profit-generating item sets from the transactional data set by performing the calculations using the quantity that is purchased, total cost and unit gain of each item in the database. The concept of time cubes implemented here helps to efficiently deal with the temporal parts of the transactional data set. Considering total cost decides the frequent customer of particular product set. The proposed system is mainly applicable in online markets, FMCG Sectors, large retail stores, and manufacturing plants for improving the revenue by promoting the profit-generating item sets.

Published in: 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)

Date of Conference: 19-20 March 2021

DOI: 10.1109/ICACCS51430.2021.9441949

Date Added to IEEE *Xplore*: 03 June 2021

Publisher: IEEE

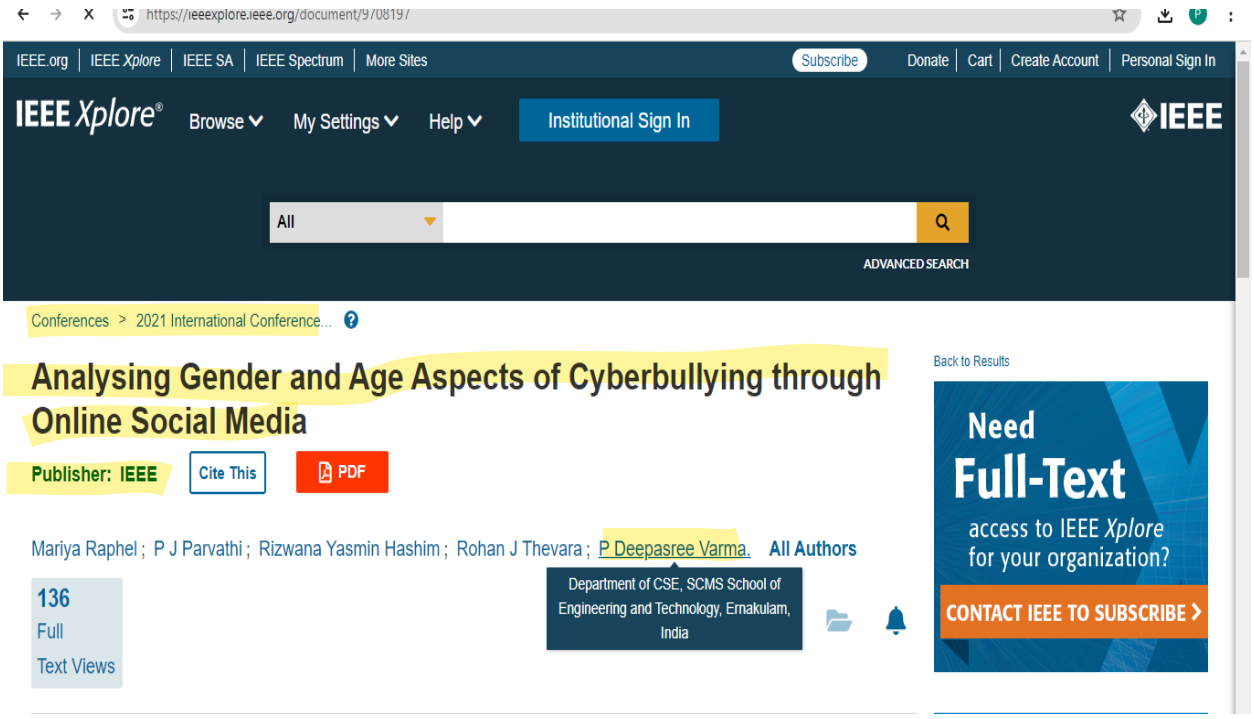
ISBN Information:

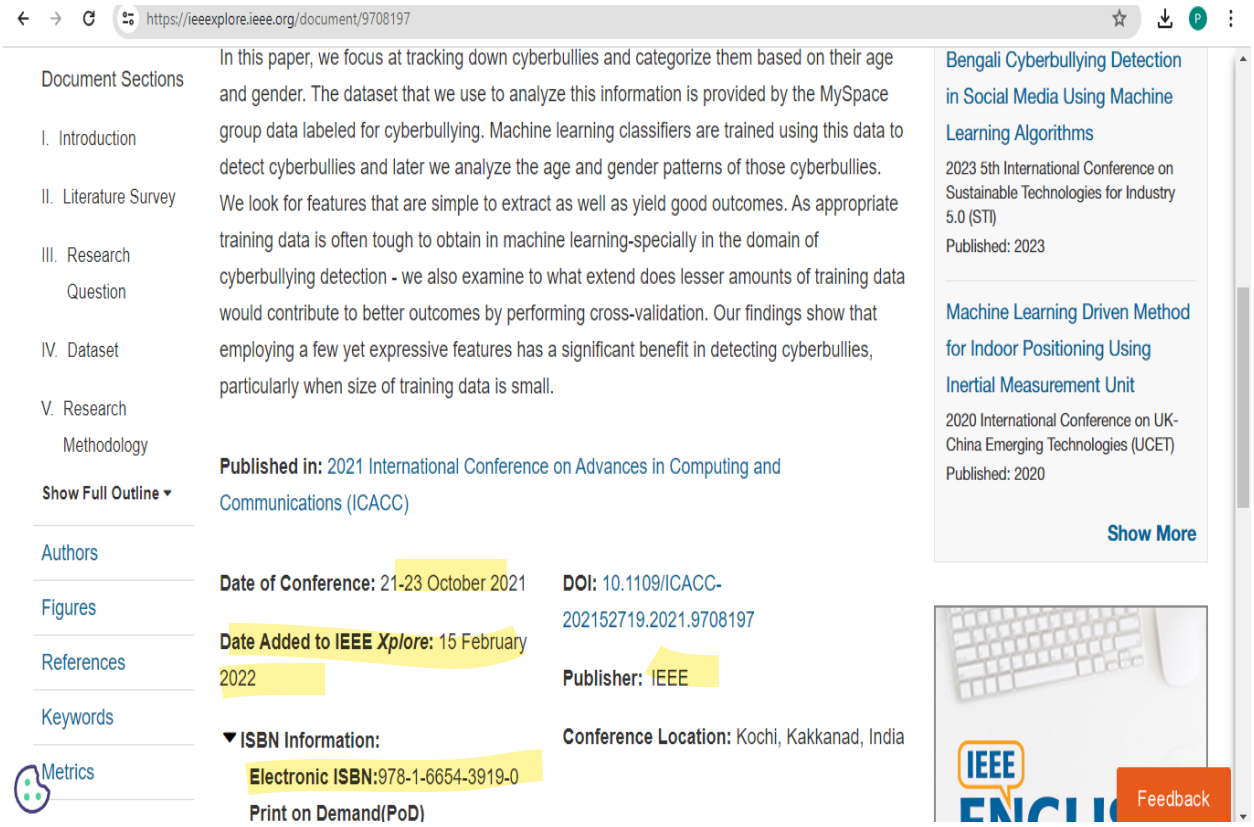
Electronic ISBN:978-1-6654-0521-8

Print ISBN:978-1-6654-0520-1

DVD ISBN:978-1-6654-0519-5

Conference Location: Coimbatore, India


https://ieeexplore.ieee.org/document/9708197
IEEE.org | IEEE Xplore | IEEE SA | IEEE Spectrum | More Sites
Subscribe
Donate | Cart | Create Account | Personal Sign In
IEEE Xplore
Browse
My Settings
Help
Institutional Sign In
IEEE
All
ADVANCED SEARCH
Conferences > 2021 International Conference...
Analysing Gender and Age Aspects of Cyberbullying through Online Social Media
Publisher: IEEE
Cite This
PDF
Mariya Raphel ; P J Parvathi ; Rizwana Yasmin Hashim ; Rohan J Thevara ; P Deepasree Varma. All Authors
Department of CSE, SCMS School of Engineering and Technology, Ernakulam, India
136
Full
Text Views
Back to Results
Need
Full-Text
access to IEEE Xplore for your organization?
CONTACT IEEE TO SUBSCRIBE


https://ieeexplore.ieee.org/document/9708197
Document Sections
I. Introduction
II. Literature Survey
III. Research Question
IV. Dataset
V. Research Methodology
Show Full Outline
Authors
Figures
References
Keywords
Metrics
In this paper, we focus at tracking down cyberbullies and categorize them based on their age and gender. The dataset that we use to analyze this information is provided by the MySpace group data labeled for cyberbullying. Machine learning classifiers are trained using this data to detect cyberbullies and later we analyze the age and gender patterns of those cyberbullies. We look for features that are simple to extract as well as yield good outcomes. As appropriate training data is often tough to obtain in machine learning-specially in the domain of cyberbullying detection - we also examine to what extend does lesser amounts of training data would contribute to better outcomes by performing cross-validation. Our findings show that employing a few yet expressive features has a significant benefit in detecting cyberbullies, particularly when size of training data is small.
Published in: 2021 International Conference on Advances in Computing and Communications (ICACC)
Date of Conference: 21-23 October 2021
Date Added to IEEE Xplore: 15 February 2022
DOI: 10.1109/ICACC-202152719.2021.9708197
Publisher: IEEE
Conference Location: Kochi, Kakkanad, India
ISBN Information:
Electronic ISBN:978-1-6654-3919-0
Print on Demand(PoD)
Bengali Cyberbullying Detection in Social Media Using Machine Learning Algorithms
2023 5th International Conference on Sustainable Technologies for Industry 5.0 (STI)
Published: 2023
Machine Learning Driven Method for Indoor Positioning Using Inertial Measurement Unit
2020 International Conference on UK-China Emerging Technologies (UCET)
Published: 2020
Show More
IEEE
Feedback

Downsampling Attack on Automatic Speaker Authentication System

Asha S
Dept.of Computer Science and Engineering
SCMS School of Engineering & Technology
Ernakulam, India
Affiliated to APJ Abdul Kalam Technological University
Trivandrum, India
ashas@scmsgroup.org

Vinod P
Dept of Computer Applications
Cochin University of Science and Technology
Cochin, India
vinod.p@cusat.ac.in

Varun G Menon
Dept.of Computer Science and Engineering
SCMS School of Engineering & Technology
Ernakulam, India
Affiliated to APJ Abdul Kalam Technological University
Trivandrum, India
varunmenon@scmsgroup.org

Akka Zemmari
Bordeaux Laboratory of Research in Computer Science
Bordeaux INP, CNRS, UMR 5800
University of Bordeaux, Bordeaux
France
zemmari@u-bordeaux.fr

***Abstract*—Recent years have observed an exponential growth in the popularity of audio-based authentication systems. The benefit of a voice-based authentication system is that the person need not be physically present. Voice biometric system provides effective authentication in various domains like remote access control, authentication in mobile applications, customer care centers for call attests. Most of the existing authentication systems that recognize speakers formulate deep learning models for better classification. At the same time, research studies show that deep learning models are highly vulnerable to adversarial inputs. A breach in security on authentication systems are not generally acceptable. This paper exposes the vulnerabilities of audio-based authentication systems. Here, we propose a novel downsampling attack to the speaker recognition system. This attack can effectively trick the speaker recognition framework by causing inaccurate predictions. The proposed threat model achieved remarkable attack effectiveness of 75%. This system employs a custom human voice dataset recorded in real-time conditions to achieve real-time effectiveness during classification. We compare the attack accuracy of the proposed attack against the adversarial audios generated using the CleverHans toolbox. The proposed attack being a black box attack, is transferable to other deep learning systems also.**

***Index Terms*—Automatic Speaker Recognition System, Voice Authentication, Adversarial Attack, Sampling Attack, Cleverhans, MFCC, Adversarial Machine Learning**

I. Introduction

Recent research trends witnessed tremendous advancement in the area of voice authentication. Nowadays various applications such as smart speakers, personal digital assistants, biometric frameworks, and forensics, enforce voice-based commands for authentication. Voice biometric system is more convenient to use as it is a contactless means of authentication. Voice biometric system incorporates identifying the human voice and finally verifying the speaker of the audio. As the use of voice-command-based applications are increasingly rising, the need to endorse security in such systems has become a demanding issue. The limitations in uniquely recognizing the owner of the voice brings the possibility of malpractices. Any person who is aware of specific voice commands can operate such systems. Hence these voice-command-based systems should also incorporate a voice recognition system that identifies and verifies genuine speakers from voice.

Automatic speaker recognition (ASR) is the challenging task of authenticating an individual's identification using voice biometrics. Fig 1 shows the typical architecture of an ASR framework. An ASR system [1] involves speaker identification and speaker verification. It collects voice samples from authentic speakers, extracts the audio characteristics, and trains the deep learning model using the extracted audio features. Speaker identification determines the identity of the speaker from the set of registered users. Speaker verification allows or denies the claim of the given speaker. Recent updates in Apple Siri [2] have made it reliably recognize voices, enabling Home Pod to respond to queries from multiple users even in shared spaces. Enterprises have started using speaker recognition technologies for authentication and authorization purposes even without them being physically present.

The speaker recognition system has attained sufficient credibility with the advent of deep learning-based classification techniques. Deep learning approaches have brought efficient scalability in human audio recognition systems. State of the art speaker recognition system has revealed that deep learning-based solutions have an extraordinary improvement over

978-1-6654-0969-8/21/$31.00 ©2021 IEEE

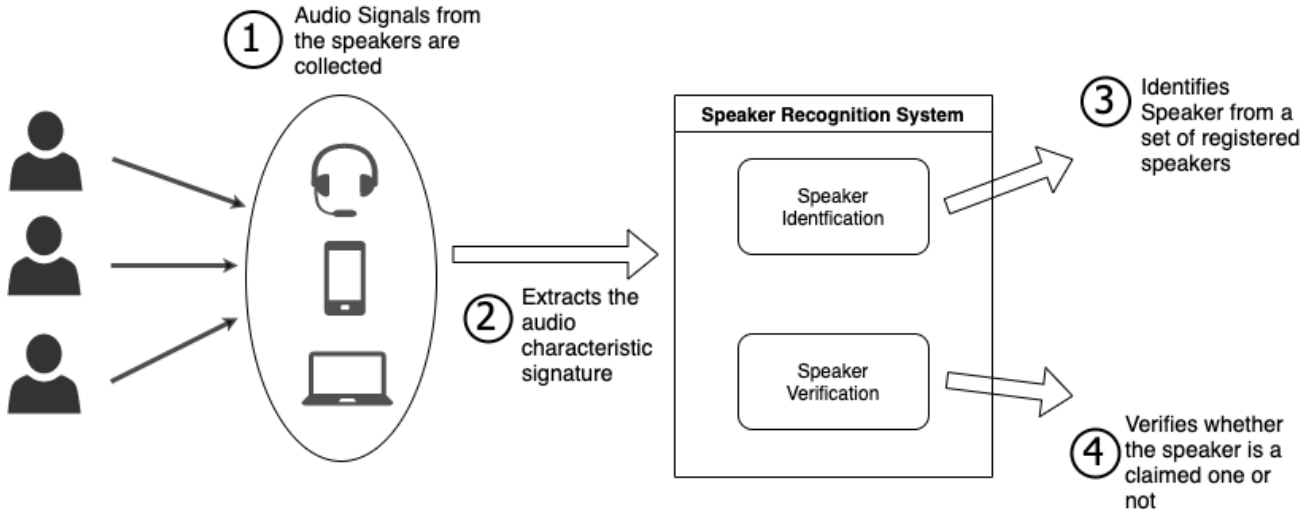


Fig. 1. Automatic Speaker Recognition System

legacy statistical approaches. On the contrary, deep learning models exhibit vulnerabilities to adversarial or perturbated inputs. Carline *et al.*[3] recently illustrated that by adding a hidden disturbance, an attacker could drive the automatic speech recognition (ASR) framework to misrecognize a voice command as any adversary-desired command. Fraudulent attacks on such systems can cause security breaches. CommanderSong [4] embeds malicious instructions into music, making individuals treat them as regular ones, though ASR systems would identify them as instructions and carry them out accordingly. These instances prove how crucial it is to have a robust speaker recognition system on top of voice-command-based applications.

Adversarial Machine Learning (AML) is the area of study that focuses on identifying the vulnerabilities in machine learning models. Adding a slight perturbation to the input data reveals the reliability of the classification model. A perturbated input datum is called an adversarial sample/input. These perturbations are often undetectable to humans. Such adversarial perturbation often fools the learned machine learning models and ultimately compromises system security. The presence of perturbated data in deep learning models causes the system to classify the input incorrectly. Fig 2 depicts a real-world scenario where the precision and efficiency of the speaker recognition framework is adversely affected by extraneous sounds. In this scenario, an authentic individual tries to open and access his mobile device, enabled by the speaker recognition framework. Disturbances in the noisy environment gets superimposed with his voice and cause a misclassification in the ASR system leading to authentication failure.

Having sound speaker recognition models that are not sensitive to adversarial disturbance is a necessity. This paper discusses a text-independent speaker recognition framework. We construct an experimental deep learning-based multi-class speaker recognition system that can identify the voice characteristics of multiple authentic speakers. We examine the robustness of our solution by exploring the feasibility of performing an over-the-air adversarial attack with the help of custom noise clips taken from youtube. Further, we evaluate the system using vulnerable samples created utilizing the CleverHans Toolbox [5]. Finally, the system introduces a novel adversarial attack called the Downsampling attack, where a downsampled target audio is embedded into the source audio to cause a misclassification. The experimentation results reveal that attaching an imperceptible perturbation into the original audio misleads the speaker recognition system.

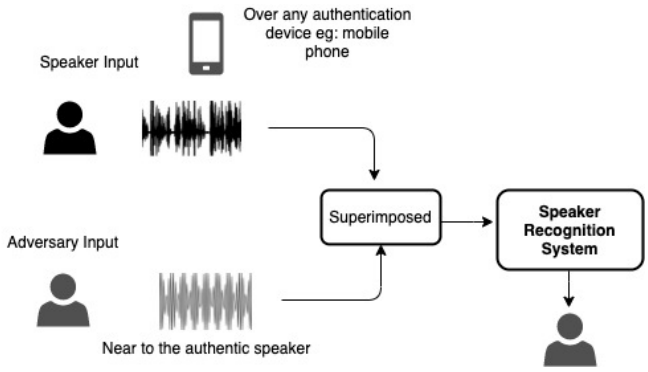


Fig. 2. Effect of Adversary on Speaker Recognition System

The rest of the paper is organized as: Section 2 gives a brief outline and taxonomy of different adversarial attacks and defenses performed on ASR systems. Section 3 discusses the proposed speaker recognition system architecture and the novel downsampling threat model. Section 4 presents the results after applying the proposed attack on the ASR system. Section 5 concludes the work by discussing the future scope of this research.

II. Literature Review

This section presents an overview of various existing adversarial attacks on ASR systems. In addition to the attack scenarios, this section also describes the potential defense strategies. Various attacks on speaker recognition systems [2] can be categorized as:

- Replay attack [6]: Employs prerecorded/ replayed voice instructions of a genuine target speaker to deceive the speaker recognition framework.
- Speech synthesis attack [7]: Speech synthesis is the artificial generation of human speech. It fabricates a victim's voice by studying an acoustic pattern from a confined set of voice samples.
- Impersonation attack [8]: An adversary could impersonate a victim's voice through mimicry by manipulating actual voice samples from genuine clients.
- Voice Conversion attack [9]: Transform the speech of a (reference) speaker so that it sounds like the speech of a different (target) speaker.

A. Adversarial Attacks

Li *et al.* in [10] proved that an i-vector [11] based speaker verification framework is responsive to adversarial attacks. This system also explains the transferability of adversarial samples generated with the i-vector system to a DNN-based x-vector [12] system. The system performs a Fast Gradient Sign Method (FGSM) [13] attack on the feature space.

Kreuk *et al.* [14] demonstrated the helplessness of an end-to-end DNN-based speaker recognition framework to FGSM assault. Here the authors perform attack perturbations on the feature space. This system also evaluates the cross-feature transferability of the attack. The paper does not suggest any defense strategy against FGSM attacks.

A Natural Evolution Strategy (NES) based adversarial sample generation strategy was introduced by Chen *et al.* in [15]. This attack could successfully counterfeit both the GMM-UBM and the i-vector [11] speaker recognition systems. They could achieve noteworthy attack effectiveness using their proposed method. During testing, they included only five speakers in the test set. To effectively evaluate the robustness of the system, more speakers could have been included in the test set.

Wang *et al.* in [16], exploit the x vector-based speaker recognition system by performing targeted adversarial attacks. The system produces imperceptible adversarial perturbations by achieving targeted white-box assaults to the speaker recognition framework. The attack targeted altering the psychoacoustic principle of frequency masking. They construct the audio adversary by masking the threshold of the original sound. This approach yields an attack accuracy of up to 98.5%.

Abdullah *et al.* in [17] constructed adversarial samples based on gradient information. They have worked with almost all white box attack strategies discussed in literature [18]. They have implemented the attack mechanism in various attack mediums like over the line, over the air, over the telephony, and others. Tianyu Du *et al.* in [19] introduces a new class of attack named SirenAttack to generate perturbated voice samples. SirenAttack uses the gradient-based method to create perturbated input and optimize it by using the Particle Swarm Optimization (PSO) algorithm.

The majority of existing adversarial attacks against the speaker recognition, construct diverse adversary perturbations for each input. To make the real-time adversary sample effective in [20], Yi Xie *et al.* construct a single universal perturbation. The advantage is that the universal disturbance can be applied straightforwardly to any speaker's articulation. Since the perturbation is universal, it also helps to reduce the attack initiation time.

B. Defenses

Wang *et al.* [21] proposed a regularization-based adversarial defense strategy that utilizes both FGSM and Local Distributional Smoothness (LDS) [22] strategy. The proposed method causes an improvement in the performance of the speaker verification framework. FGSM was the only attack employed in the system. This attack is conducted on the feature space and not on the time domain.

Wu *et al.* proposed two defensive strategies in [23], a passive defense method and a proactive method. Passive method aims to counter adversarial assaults without altering the model. Here, the model makes use of the spatial smoothing method. Proactive defense techniques equip new models which are robust to adversarial instances. The system in [23] uses a proactive defense strategy comparable to adversarial training.

A Liveness Detection defense approach is proposed by Abdullah *et al.* in [17] along with adversarial training. It points to distinguish whether the source of discourse was a genuine human or a mechanical speaker. It offers support to avoid replay sound assaults.

III. Speaker Recognition System

This section comprises two subsections. The former explains the architecture of the multi-class speaker recognition system constructed for evaluation, and the latter illustrates the proposed downsampling threat model.

A. Target Speaker Recognition Model

Fig. 3 depicts the architecture of our speaker recognition system. The system makes use of a deep learning-based network for speaker identification. The proposed system is a text-independent identification system. It trains the network using audio samples from a custom dataset that can accurately classify twenty speakers. For efficient classification performance, the system extracts and makes use of the Mel Frequency Cepstral Coefficient (MFCC) [24] feature vector. In the verification phase, the trained speaker recognition model classifies the feature vector of the test speaker as genuine or an imposter.

Architecture under study involves three processes: Frontend Processing, Feature Extraction, and Training the Model.

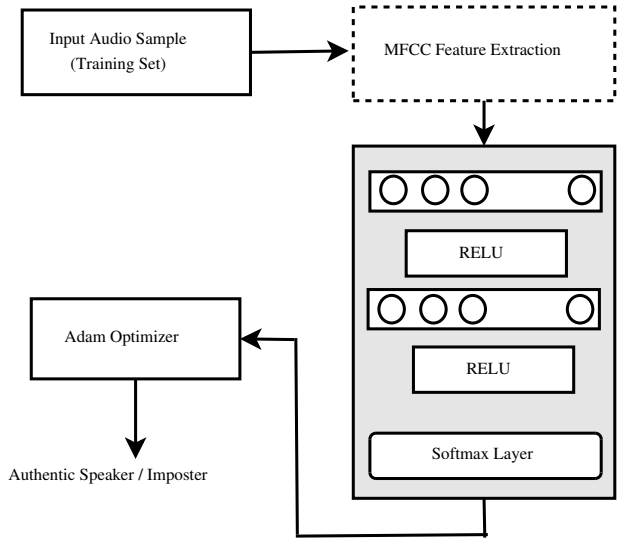


Fig. 3. Proposed System Architecture

- Frontend processing removes non-speech portions from the signal.
- The feature extraction process extracts the speaker information trait from the input signal. The extracted feature further undergoes channel compensation.
- During the training phase, a sequential model is adopted to perform the feature training.

Preprocessing step disposes of the periods whose signal energy falls underneath a specific threshold limit. It is typically a noise reduction stage that identifies portions of sound containing human speech. The system uses Butterworth high pass filter with a cutoff frequency of 1000 Hz. Expelling such unnecessary noise from the audio samples helps to improve ASR accuracy.

The feature extraction phase splits the preprocessed audio into short frames and extracts characteristic features from each. The most commonly used trait in voice processing systems is MFCC [24]. Extracting MFCC features includes changing the sound to the frequency domain via a Discrete Fourier Transform, followed by implementing a Mel Filter Bank, and then performing a reverse fourier transform to switch the signal back to the time-space.

To compensate for long-term spectral effects caused by different microphones and audio channels, standard techniques such as Cepstral mean normalization (CMN) and variance normalization (CVN) are employed. The CMN subtracts the mean vector from each input frame, CVN will normalize the variance. When CMN and CVN are enabled, features get normalized to $N(0, 1)$.

Our system devised a sequential model for building the speaker recognition system. The model employs three layers; the first layer has an input shape of size 40 with 256 dense units, the second has 256 dense units and the output layer with 4 dense units with softmax as an activation function. In the context of multi multiclass classification, the softmax layer delivers genuine probability values. The Adam optimizer is used to train your network, which operates efficiently on noisy and sparse data.

B. The Proposed Threat Model

The speaker recognition system F can be mathematically formulated as: Given a training set $(S_i, C_i); 1 \leq i \leq n$ of speech utterances, where S_i denotes the input feature vector and C_i denotes the corresponding output speaker label to F. During training, for each given S_i the system F learns to classify it into the corresponding speaker class C_i. Thus the learning formulates the mapping

$$F(S_i) = C_i; \quad i \in [1, n] \tag{1}$$

An adversary tries to create a perturbated audio sample S_i^* which is similar to input feature vector S_i; $S_i^* \simeq S_i$, when given to the trained system, gets misclassified as

$$F(S_i^*) = C_j; \quad C_j \in C_i \quad and \quad i \neq j \tag{2}$$

for a few or all S_i^*

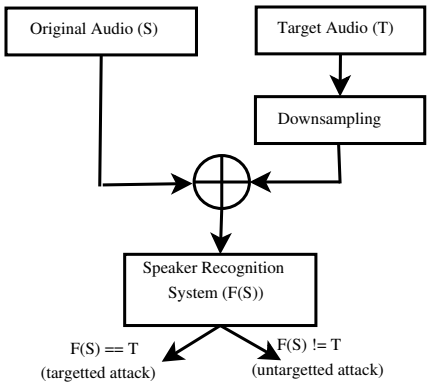


Fig. 4. Downsampled attack model on Audio

The proposed threat model is a played over-the-air black box attack strategy, where the adversary is unaware of the details of the classification model. Fig 4 depicts the downsampling threat model. The adversary crafts an attack by randomly choosing a pair of utterances from the given set of speaker utterances C. Let the source speaker audio be S, and target speaker audio be T. The target speaker audio must be different from the source speaker audio. The adversary initially downsamples the target speaker audio by a factor d (downsampling by 1/2, 1/3, 3/4, 1/4) and produces T_d. It then overlays the downsampled target audio T_d with the source speaker audio S to generate the adversary sample S^*. The adversary can perform either a targeted attack or an untargeted attack.

$$F(S^*) = \begin{cases} F(T) & \text{if } targettedattack \\ F(T^*), T^* \neq S & \text{if } untargettedattack \end{cases} \tag{3}$$

In a targeted attack, the adversary sample causes the recognition system to misclassify it into a specific target speaker $F(S^*) = F(T)$. In an untargeted attack, the adversary input causes the system to output any speaker other than the

source speaker $F(S^*) \neq F(S)$.

IV. Results and Discussions

A. Dataset

Most of the available datasets for speaker recognition endure one or more of the following shortcomings; (i) the audio files in these datasets are recorded under controlled conditions, (ii) they have restrictions in the size of the audio, (iii) not readily accessible to the speaker community. Moreover, to develop a speaker authentication system for handheld devices like smartphones and PDA, the system needs to be trained with real-time human speeches instead of celebrity voices or any other prerecorded datasets. We compiled a customized dataset to circumvent these restrictions and achieve real-time efficiency when authenticating.

Our custom dataset comprises audio samples of 10 speakers identified as Speaker 1, Speaker 2, up to Speaker 10. An average of 50 audio samples from each speaker is taken, making 500 audio samples in total. Speakers 4, 5, 6, 7, and 9 are females, and the rest are males. The recordings have been performed under uncontrolled recording settings to make the data set harder and sounder. The audio samples are captured in diverse natural conditions and under different climatic conditions. The duration of each record varies between 3 and 8 seconds. The test data set includes 100 audios from the speakers above.

To evaluate the strength of our speaker recognition system, we have picked five types of unfavorable noise with varying properties from Youtube, namely the rain, bus station, children's playing, cars, and crowds on the market. Five noises were acquired for each category, a total of 25 adversary noises.

B. Experimental Outcome

This subsection evaluates the robustness of our speaker recognition system with and without the presence of the adversary.

Evaluation Metric: The classification accuracy is calculated as accuracy = $(N_s/N_a) * 100\%$, where N_a is the total number of test audio samples, and N_s is the number of audio examples that are correctly transcribed.

Table I shows the classification accuracy of our speaker recognition system. It represents the accuracy gained during the training, validation, and testing phase. The system is assessed by using the test dataset comprising of 100 audios. We gathered ten audios from each speaker under several uncontrolled settings. The system exhibits a training and validation accuracy of 91.26% and 98.08%. When introduced with random input utterances, our system exhibits a few misclassifications resulting in a classification precision of 88%.
.

Robustness Analysis: The robustness of the experimental speaker recognition system is evaluated using (i) the proposed downsampling threat model (ii) adding five types of adversarial noises to the recordings in the custom dataset.

TABLE I
Classification Accuracy of our Speaker Recognition System

Training Accuracy (%)	**Validation Accuracy** (%)	**Test Accuracy** (%)
91.26	98.08	88

(iii) adversarial audio crafted using CleverHans tool. Table II presents the overview of the classification accuracy of all three attack strategies.

TABLE II
Classification Accuracy of Speaker Recognition System under various adversarial conditions.

Attack Category	**#Samples**	**Adversary Sample/Type**	**Classification Accuracy**
Adversarial Noise	500	Rain Noise	50
	500	Bus Station	50
	500	Market Crowd	78
	500	Roadside vehicle	81
	500	Kids Playing	50
CleverHans	100	FGSM	28
	100	BIM	48
	100	JSMA	50
	100	LBFGS	36
	100	CW	50
Proposed Threat Model	100	**Downsampling Attack**	**25**

To efficiently assess the effectiveness of our proposed threat model, we considered different downsampling rates (3/4, 1/2, 1/3, and 1/4). A downsampling rate of 1/4 indicates a reduction in the sampling rate of target audio by a factor of 1/4. This downsampled audio is then overlaid with the source audio and sent to the ASR system for evaluation. The attack effectiveness of the system at different downsample rates is demonstrated in Fig 5. Here we choose four random speakers (speakers 1, 2, 3, 4) only. The precision of the attack at a downsampling rate of 3/4 is very high. The efficiency of the threat model diminishes with the increasing degree of sampling. At a lower downsampling rate, the obtained superimposed audio becomes perceptible to the users. We eventually arrived at a downsampling rate of 1/3 as it provides fair attack effectiveness of 75% keeping the hostile audio obscure to the third person.

We compare our proposed downsampling threat model with the other two attack strategies; (i) adversarial noise taken from youtube (ii) adversarial voice generated using CleverHans tool. We have overlaid every audio in the test dataset with 25 adversarial sounds to measure the influence of an opponent's audio. This process produces a total of 2500 (25 x 100 = 2500) samples, .i.e 500 adversary audio for each adversary noise category. Table II shows that the roadside noise of vehicles has less impact on the classification. Similarly, market

crowd adversary noise attained a classification accuracy of 78%. The other three adversarial noises (rain, bus station, and kids playing) have reduced the classification accuracy to 50%. From Table II, the addition of several adverse sounds from youtube results in a precision decrease of 88 % percent to an average of 61.8 %.

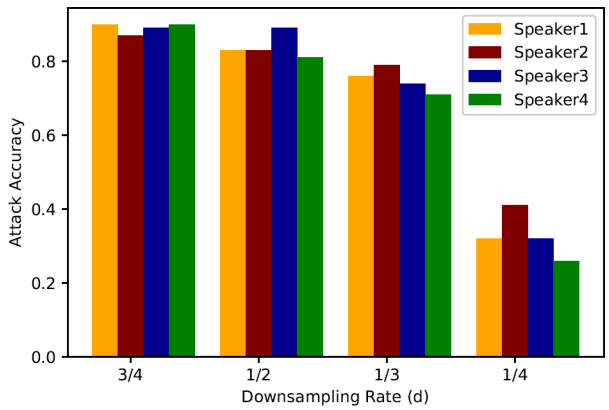


Fig. 5. Attack Accuracy of different downsampling rate on 4 Speakers

TABLE III
ATTACK ACCURACY ON TARGETTED AND UNTARGETTED ATTACK

Attack	Attack Type	Attack Accuracy
Downsampling Attack	Targetted	67
	Untargetted	75

We compared the proposed threat model against attacks implemented using CleverHans Toolbox. State-of-the-art studies on adversarial tools state that CleverHans produces better attack results compared to other toolboxes. CleverHans implements a total of 16 disruptions, including Fast Gradient Method (FGSM), Carlini&WagnerL_2 (CW), Basic Iterative Method (BIM), Projected Gradient Descent, Jacobian Saliency Map Attack (JSMA), DeepFool, Elastic Net, and L-BFGS. On each of the 100 test audio, the most popular and effective attack methods like FGSM, BIM, JSMA, L-BFGS, and CW were performed and analyzed. Table II summarizes that FGSM yields the lowest classification accuracy (28%) compared to the other four attack methods. It shows that FGSM gives a higher attack accuracy and JSMA and CW methods exhibit the lowest.

The average classification accuracy of our proposed downsampling attack method is 25% shown in Table II. The attack effectiveness of the downsampling attack is higher compared to the other attack categories. We evaluated the downsampling attack effectiveness for both targetted and untargeted speakers. Targetted attack effectiveness deals with how effectively the system can recognize the speaker of the target audio. The efficacy of an untargeted attack shows how accurately the system causes a misclassification. The proposed threat model gives higher attack effectiveness for untargeted attacks compared to targetted attacks. Table III shows that the attack accuracy is 67% for the targeted attack, and the untargeted attack is 75% accurate.

V. CONCLUSION

This paper proposes an effective and imperceptible adversarial attack on Speaker Recognition System. The downsampling attack being black box in nature will be transferable to other types of classification systems also. The transferability of this attack needs to be further explored. From the experimental analysis, we observe that the proposed attack provides reasonable attack effectiveness compared to the traditional method of generating noise. We also found it more effective than the adversarial audio generated by CleverHans tool. The proposed attack method can also be extended further by studying the impact of upsampling on the source audio. Also, it is worth exploring the possibilities of practical defenses for such an attack.

REFERENCES

[1] J. P. Campbell, "Speaker recognition: A tutorial," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1437–1462, 1997.

[2] Z. Li, C. Shi, Y. Xie, J. Liu, B. Yuan, and Y. Chen, "Practical adversarial attacks against speaker recognition systems," in *Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications*, 2020, pp. 9–14.

[3] N. Carlini and D. Wagner, "Audio adversarial examples: Targeted attacks on speech-to-text," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 1–7.

[4] X. Yuan, Y. Chen, Y. Zhao, Y. Long, X. Liu, K. Chen, S. Zhang, H. Huang, X. Wang, and C. A. Gunter, "Commandersong: A systematic approach for practical adversarial voice recognition," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 49–64.

[5] N. Papernot, F. Faghri, N. Carlini, I. Goodfellow, R. Feinman, A. Kurakin, C. Xie, Y. Sharma, T. Brown, A. Roy, A. Matyasko, V. Behzadan, K. Hambardzumyan, Z. Zhang, Y.-L. Juang, Z. Li, R. Sheatsley, A. Garg, J. Uesato, W. Gierke, Y. Dong, D. Berthelot, P. Hendricks, J. Rauber, and R. Long, "Technical report on the cleverhans v2.1.0 adversarial examples library," *arXiv preprint arXiv:1610.00768*, 2018.

[6] P. Kemanth, S. Supanekar, and S. G. Koolagudi, "Audio replay attack detection for speaker verification system using convolutional neural networks," in *International Conference on Pattern Recognition and Machine Intelligence*. Springer, 2019, pp. 445–453.

[7] Z. Wu, E. S. Chng, and H. Li, "Detecting converted speech and natural speech for anti-spoofing attack in

speaker recognition," in *Thirteenth Annual Conference of the International Speech Communication Association*, 2012.

[8] C. Parampalli, R. Sekar, and R. Johnson, "A practical mimicry attack against powerful system-call monitors," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, 2008, pp. 156–167.

[9] Z. Wu and H. Li, "Voice conversion and spoofing attack on speaker verification systems," in *2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference*. IEEE, 2013, pp. 1–9.

[10] X. Li, J. Zhong, X. Wu, J. Yu, X. Liu, and H. Meng, "Adversarial attacks on gmm i-vector based speaker verification systems," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 6579–6583.

[11] N. Dehak, P. J. Kenny, R. Dehak, P. Dumouchel, and P. Ouellet, "Front-end factor analysis for speaker verification," *IEEE Transactions on Audio, Speech, and Language Processing*, pp. 211–252, 2010.

[12] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, "X-vectors: Robust dnn embeddings for speaker recognition," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2018, pp. 5329–5333.

[13] G. Ian, J. Shlens, and S. Christian, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014.

[14] F. Kreuk, Y. Adi, M. Cisse, and J. Keshet, "Fooling end-to-end speaker verification with adversarial examples," in *2018 IEEE International Conference on Acoustics Speech and Signal Processing*. IEEE, 2018, pp. 1962–1966.

[15] G. Chen, S. Chen, L. Fan, X. Du, Z. Zhao, F. Song, and Y. Liu, "Who is real bob? adversarial attacks on speaker recognition systems," *arXiv preprint arXiv:1911.01840*, 2019.

[16] Q. Wang, P. Guo, and L. Xie, "Inaudible adversarial perturbations for targeted attack in speaker recognition," *arXiv preprint arXiv:2005.10637*, 2020.

[17] H. Abdullah, K. Warren, V. Bindschaedler, N. Papernot, and P. Traynor, "Sok: The faults in our asrs: An overview of attacks against automatic speech recognition and speaker identification systems," *arXiv e-prints*, pp. arXiv–2007, 2020.

[18] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, 2013.

[19] T. Du, S. Ji, J. Li, Q. Gu, T. Wang, and R. Beyah, "Sirenattack: Generating adversarial audio for end-to-end acoustic systems," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 357–369.

[20] Y. Xie, C. Shi, Z. Li, J. Liu, Y. Chen, and B. Yuan, "Real-time, universal, and robust adversarial attacks against speaker recognition systems," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 1738–1742.

[21] Q. Wang, P. Guo, S. Sun, L. Xie, and J. H. Hansen, "Adversarial regularization for end-to-end robust speaker verification," *In Interspeech*, pp. 4010–4014, 2019.

[22] T. Miyato, S. ichi Maeda, M. Koyama, K. Nakae, and S. Ishii, "Distributional smoothing with virtual adversarial training," *arXiv preprint arXiv:1507.00677*, 2015.

[23] H. Wu, S. Liu, H. Meng, and H.-y. Lee, "Defense against adversarial attacks on spoofing countermeasures of asv," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 6564–6568.

[24] D. O'Shaughnessy, "Automatic speech recognition: History, methods and challenges," *Pattern Recognition*, vol. 41, no. 10, pp. 2965–2979, 2008.

2021 8th International Conference on Smart Computing and Communications (ICSCC)

A Study on the Effect of Hardware Trojans in the Performance of Network on Chip Architectures.

Josna Philomina
Department of Computer Science and Engineering
SCMS School of Engineering and Technology
Ernakulam, India
josnaphilomina@scmsgroup.org

Abstract **-Network on chip (NoC) is the communication infrastructure used in multicores which has been subject to a surfeit of security threats like degrading the system performance, changing the system functionality or leaking sensitive information. Because of the globalization of the advanced semiconductor industry, many third-party venders take part in the hardware design of system. As a result, a malicious circuit, called Hardware Trojans (HT) can be added anywhere into the NoC design and thus making the hardware untrusted. In this paper, a detailed study on the taxonomy of hardware trojans, its detection and prevention mechanisms are presented. Two case studies on HT-assisted Denial of service attacks and its analysis in the performance of network on Chip architecture is also presented in this paper.**

Keywords— Multicore, Network on Chip (NoC), Hardware Trojans (HT), Tiled Chip Multicore Processors (TCMP).

I. INTRODUCTION

Mobiles and handheld devices are becoming part and parcel of our day today life. More number of applications have to be executed concurrently and the performance of the device cannot be compromised at any level. Also, we are living in the era of machine learning where more computation intensive tasks have to be performed. In all these scenarios the prior requirement is that performance of the processor must be high enough to get the expected work done.

With the advancement of VLSI technology, a greater number of transistors can be accommodated in a single chip which give rise to more advanced processors. But the performance of unicore processor is limited by frequency wall, power wall, Instruction Level Parallelism (ILP) wall and Memory wall. In order to improve the performance further we need a paradigm shift from unicore processor to multicore processor. Instead of a single faster processor use multiple slower processors to do a task and achieve very high performance. This is the main idea behind multicore architectures. Multicore architecture consists of a single chip with multiple processing elements and associated cache memories.

A core consists of a control unit, registers and functional unit. Main memory and the disk are placed outside the core and a bus interface is used to communicate between different processing elements. Fig 1 shows single core chip architecture and Fig 2 shows multi core chip architecture.

In Fig. 1, a single CPU chip is connected to the bus interface whereas in Fig. 2, multiple CPU chips are connected to bus interface. But when a greater number of cores are included in a single chip, bus-based interconnection mechanism become a bottleneck. Then it needs a paradigm shift from bus-based interconnection mechanism to Network based interconnection mechanism. Network on Chip (NoC) is the communication infrastructure used in multicore architectures. In multicore architectures, all processing elements (PE) are organized in matrix format where each PE is called as a Tile. Each tile has an address (x, y), where x denotes the row number

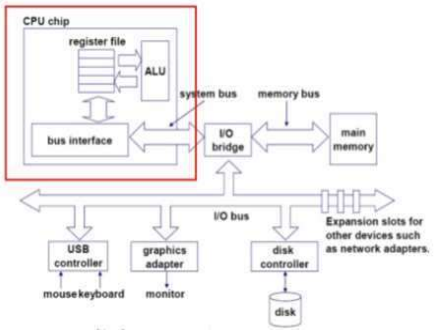


Fig. 1 Single core computer

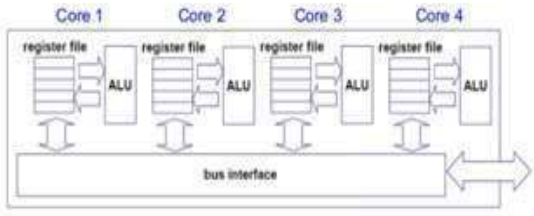


Fig. 2 Multi core CPU Chip

and y denote the column number. The numbering starts from top left corner and then to the right. This type of organization is called as Tiled chip multiprocessing (TCMP). PEs are interconnected by network of routers, where the routers are the communication backbone in TCMP.PEs communicate with each other with the help of packet-based network. Each packet consists of data part and overhead part. Data part contains data and overhead part contains source address, destination address, sequence number etc. Each packet is divided into flow control units called flits which is the smallest unit of flow control in the Network on chip architectures.

Several attacks can happen in the communication infrastructure that can degrade the system performance. To improve the reliability of the system and degrade the attack, runtime detection methods and mitigation mechanisms are explored by researchers as

978-1-7281-9687-9/21/$31.00 ©2021 IEEE

other machine learning techniques to estimate age of a person from fingerprints and also spoof detection. The models we compare include three pre-trained CNNs which are fine-tuned with the fingerprint images, and a classical Local Binary Pattern approach. It is found that pre-trained CNNs along with Dataset Augmentation can produce good results with no need for any hyperparameter selection. NIST dataset was used for age detection and LiveDet 2013 dataset was used for spoof detection. It was able to achieve a top accuracy of 84% for age detection and 94% for spoof detection. The paper also focuses on identifying the best scanner for our purposes and also the possible materials used for spoofing.

Published in: 2021 International Conference on Advances in Computing and Communications (ICACC)

Date of Conference: 21-23 October 2021

DOI: 10.1109/ICACC-202152719.2021.9708286

Date Added to IEEE *Xplore*: 15 February 2022

Publisher: IEEE

ISBN Information:

Electronic ISBN:978-1-6654-3919-0

Print on Demand(PoD)

ISBN:978-1-6654-3920-6

Conference Location: Kochi, Kakkanad, India

Chapter

A Deep Learning-Based Model for an Efficient Hate-Speech Detection in Twitter

By P. R. Vishnu, Basant Agarwal, P. Vinod, K. A. Dhanya, Alice Baroni

Book Securing Social Networks in Cyberspace

Edition	1st Edition
First Published	2021
Imprint	CRC Press
Pages	16
eBook ISBN	9781003134527

Share

Video Forgery Detection using CNN

Litty Koshy ; Ashil Basheer All Authors

SCMS School of Engg. and Technology, Kochi, Kerala

video editing software has grown, so has the number of negative repercussions and risks associated with such editing procedures. By merging, changing, or synthesising new footage, video forgery is a technique for creating changed or fraudulent videos. A method based on deep learning is given in the proposed system for classifying videos as tampered or original. The video clip that is used as input is divided into two categories: original and modified. The video is segmented into non-overlapping frames, and the authenticity of the movie is determined by whether or not all of the frames are genuine. The suggested method uses a deep CNN model that has two types of layers: (1) CNN layers which involve convolutional, pooling and fully connected layers and (2) Parasitic layers.

Published in: 2021 Smart Technologies, Communication and Robotics (STCR)

Date of Conference: 09-10 October 2021

DOI: 10.1109/STCR51658.2021.9588860

Date Added to IEEE *Xplore*: 10 November 2021

Publisher: IEEE

Conference Location: Sathyamangalam, India

▼ **ISBN Information:**

Electronic ISBN:978-1-6654-1806-5

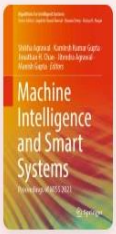
Print on Demand(PoD)

ISBN:978-1-6654-1807-2

Underwater Image Enhancement Using Fusion Stretch Method

Conference paper | First Online: 24 May 2022

pp 75–87 | Cite this conference paper



Machine Intelligence and Smart Systems

https://link.springer.com/chapter/10.1007/978-981-16-9650-3_6

Litty Koshy & Shwetha Mary Jacob

Litty Koshy

Department of CSE, SCMS School of Engineering and Technology, Ernakulam, Kerala, India

Contact Litty Koshy

View author publications

You can also search for this author in PubMed | Google Scholar

Underwater image enhancement is an effective method for improving the captured underwater images that have been damaged owing to medium dispersion and absorption. Based on the principles of fusion, this method derives the inputs and the weight maps from the image's degraded version. Two inputs representing color-corrected and contrast-enhanced versions of the original underwater image and three weight maps that seek to increase the visibility of degraded objects due to the medium dispersion and absorption are specified here to overcome the limitations of the underwater medium. This method is a single image approach that does not need specialized hardware or underwater conditions scene expertise. In order to facilitate the transfer of edges and color contrast to the

Check for updates

Cite this paper

Koshy, L., Jacob, S.M. (2022). Underwater Image Enhancement Using Fusion Stretch Method. In: Agrawal, S., Gupta, K.K., Chan, J.H., Agrawal, J., Gupta, M. (eds) Machine Intelligence and Smart Systems. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-9650-3_6

Download citation

.RIS .ENW .BIB

DOI
https://doi.org/10.1007/978-981-16-9650-3_6

Published
24 May 2022

Publisher Name
Springer, Singapore

Print ISBN
978-981-16-9649-7

Online ISBN
978-981-16-9650-3

eBook Packages
Intelligent Technologies and Robotics
Intelligent Technologies and Robotics (R0)

10 Effect of Exfoliation on Structural and Electrochemical Properties

Gibin George
SCMS School of Engineering and Technology

Deepthi Panoth
Kannur University

Brijesh K
National Institute of Technology Karnataka (NITK) Surathkal

Anjali Paravannoor
Kannur University

Nagaraja Hosakoppa
National Institute of Technology Karnataka (NITK) Surathkal

Yu-Hsu Chang
National Taipei University of Technology

Sreejesh Moolayadukkam
Centre for Nano and Soft Matter Sciences (CeNS)

CONTENTS

DOI: 10.1201/9781003178453-10

10.1 INTRODUCTION

The term exfoliation represents a process during which the layered bulk materials are expanded through a chemical or physical method to overcome the weak inter-layer forces that hold the layers together. Generally, the stacked layered materials seized together by van der Waals forces can be easily intercalated or exfoliated by solution methods or simple physical means such as shear or ultrasonic vibrations to form 2D nanosheets. The exfoliated 2D nanosheets are often composed of single or few layers of atoms, and most importantly several of their properties are largely deviated from the bulk. Such materials find applications in electronics, photonics, catalysis, supercapacitors, fuel cells, batteries, etc. [1]. The success of graphene triggered the development of other 2D structured nanomaterials, especially by the exfoliation of layered bulk inorganic materials. Unlike bulk materials, 2D nanosheet counterparts exhibit unique electron and phonon transport characteristics, which leads to several fascinating properties such as thermal conductivity, ion transport, and charge carrier concentration, besides the structural and mechanical properties.

Many of the 2D nanosheets are non-toxic and can be handled easily, and they can be cast to any substrate as a thin film for device fabrication [2]. Over the years, exfoliated 2D nanolayers have become an essential part of electrochemistry, mainly in sensing, energy, and environmental applications. 2D carbon allotropes such as graphene and 2D porous carbon are not electrochemically active by themselves; therefore, they are often doped/modified by heteroatoms such as B, P, and N or transition metals. The high charge conductivity of the 2D carbon materials is highly favorable for several electrochemical applications such as batteries, supercapacitors, sensors, and catalysis. The stability of several inorganic 2D nanosheets in acidic and basic media makes them attractive for the aforesaid applications and they are considered as the immediate replacement for expensive noble metal electrocatalysts [3].

MXenes are 2D nanolayers of metal carbides, carbo-nitrides, and nitrides, an important class of electroactive 2D nanomaterials that are developed lately. $Ti_3C_2T_x$ is the first MXene discovered in 2011. So far about 50 different types of MXenes with wide chemical and structural variations are synthesized by exfoliating MAX phases by selective etching and mechanical shearing. MAX phases represent a family of ternary carbides and nitrides. MXenes are unstable in oxygen-containing environments. The hydrophilic nature and high surface charge of MXene nanosheets make them stable in polar solutions for device printing. The ability of MXenes to intercalate various cations including multivalent ions and polar organic molecules between its 2D layers makes them apt for non-lithium-ion batteries and supercapacitors [4]. Alike graphene, MXene exhibits excellent electronic conductivity and can be functionalized, hybridized, and doped for tuning the properties to meet the requirements of a specific application.

Many non-noble metal electrocatalysts are inactive and unstable in acidic mediums. The reaction in an acidic medium is highly efficient at a high current density. Transition metal dichalcogenides (TMDs) are highly active electrocatalysts for sensing, batteries,

supercapacitor, water splitting, etc., especially in acidic and harsh environments. TMDs have the general formula MX_2, where M is the transition metal and X is the chalcogen (X = S, Se, and Te), having a similar layered structure to those of graphene. Alike any other 2D layered nanosheets, TMDs can be doped, functionalized, and hybridized for improving various operating parameters such as selectivity, sensitivity, and affordability in sensing and efficiency, stability, and life span in catalysis. Additionally, TMDs have good electronic and mechanical properties favorable for electrode materials [5].

2D nanosheet of layered hydroxides (LDHs) and oxides are also an important class of electrochemical materials, starting from sensing to fuel cells. The presence of oxyl and hydroxyl groups allows the efficient transport of ions when they are used as electrodes in energy storage. The possibility of intercalation of ions other than Li^+ makes them a promising candidate for non-lithium-ion batteries. The electronic conductivity of LDHs and oxides are poor, therefore these materials are often hybridized with carbon-containing conductive materials as an effective strategy to increase the intrinsic catalytic activity. In this chapter, the electrochemical applications of the exfoliated 2D nanosheets in batteries, supercapacitors, biological sensing, and water splitting are discussed concisely. The underlying mechanism of electrochemical activity of different classes of 2D layered nanosheets is different. Such unique characteristics of different classes of 2D nanosheets favorable for the respective applications are also explored in this chapter.

10.2 ELECTROCHEMICAL SENSORS

A large number of sensors are used in our daily life to monitor and modify ourselves and our surroundings in a positive way. Electrochemical sensors have the largest share among all the chemical sensors, which use an electrochemical reaction (parameters such as a change in current and impedance) of the analyte to quantify the concentrations. Analytes electrochemically interact with the active material to produce signals and the sites on which such interactions happen are known as electrochemically active sites. Usually, the concentration of electrochemically active surface area increases with the surface area of the active material. Interestingly, exfoliation of 2D materials increases the surface area and exposes active sites, which may not be active otherwise. Often, exfoliated materials take part in the electrochemical reaction or act as a host to molecules such as enzymes that catalyze the reaction. Exfoliation, being a top-down approach results in defects that can also have a positive influence on the electrochemical reactions because of their very high activity. Apart from this, the extend of exfoliation, lateral size, etc. is also critical in deciding exfoliated material's electrochemical activity [6].

Graphene, which is a carbon allotrope, is the first known material to be exfoliated into atomically thin layers from its bulk counterpart graphite. Graphite can be easily exfoliated by mechanical cleaving. This can be used as an advantage in sensing where the fouling of the electrode material is a serious concern. The detection of material like bisphenol-A involves the polymerization of the analyte molecules and results in the deposition of the material on the surface of the electrode, which results in the electrode fouling. Exfoliated graphite helps in tackling this issue wherein a mild polishing results in the removal of the polymerized products from the surface as described by Ndlovu et al. [7]. Figure 10.1 schematically represents how exfoliation acts as a tool to challenge the fouling issues in electrochemical sensing.

Graphite oxide samples are usually exfoliated using thermal shock to achieve high quality and are electrochemically active for the detection of hydrogen peroxide and this is extensively reported by many researchers. Moolayadukkam et al. in 2020, in detail, explained the effect of solar exfoliation on the H_2O_2 sensing performance. Exfoliated graphene sheet has more defect concentration, which acts as the electrocatalytically active sites by adsorbing the analyte molecules. These adsorbed analyte molecules are electrocatalytically oxidized and corresponding signals can be recorded with a technique such as chronoamperometry. Figure 10.2 schematically shows graphene layers with defects/pores and their activity in adsorbing H_2O_2 molecules (analyte) [8].

Non-carbonaceous materials are electrocatalytically more active and their exfoliation has revolutionized electrochemical sensing research and developments. Layered 2D TMDs offer a wide variety of materials that can be exfoliated and having electrical properties varying from metallic to semiconducting nature. The peculiar arrangement of each atomic layer in TMDs offers a variety of active sites for the analyte adsorption in each layer after the exfoliation process. This property is widely used in the efficient detection of biomolecules. MoS_2 is one of the most widely used TMDs for sensing and other applications. Ashwathi et al. studied the relation between the analyte affinity and the active material by taking MoS_2 and Hg (II) ions as an example. In this particular example, Hg (II) ions have a high affinity toward S-containing groups. Exfoliation leaves S on both the surfaces of nanosheets exposed while the Mo layer at the center acting as the backbone. This arrangement of atoms improves the sensitivity by many folds clearly showing exfoliation of 2D TMDs could be used as an effective method for fine-tuning sensing capabilities [9].

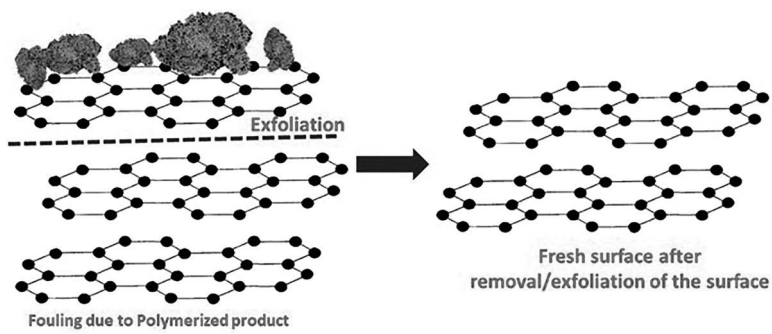


FIGURE 10.1 Shows how exfoliation of the material helps tackle the fouling issues in sensing.

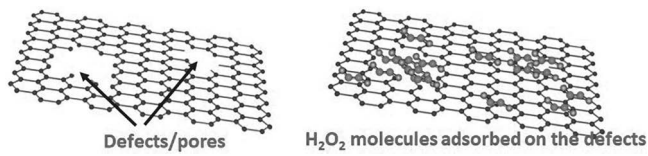


FIGURE 10.2 Schematic representation showing the importance of defects in adsorbing the analyte molecules on the graphene surface.

LDHs are another class of materials that can be exfoliated to form molecular layers with metal as the center layer. Compared to TMDs, LDHs have the advantage that there may be more than one metal in the metallic center layer, and varying the ratios of metals at the center and the metals themselves can tweak the sensing properties [10]. Sahoo et al. studied the sensing properties of ultrasonically exfoliated Ni_2Co-LDH with dopamine, an important biomolecule. The electron transfer rates are reported to be improved on moving from bulk to the monolayers of the LDH. Going from bulk to monolayers could help decrease the electron scattering at the active material, which can have a positive impact on the sensing properties [11]. Strong dependence of the exfoliation on the sensing properties is also reported by Chia et al., Authors explained the effect of exfoliation using enzymatic glucose sensing as a tool. Exfoliated 2D sheets show better sensing properties because of the high surface area and thin nature. Thinner sheets result in a decreased distance between adsorbed enzyme and the electrode, which facilitates efficient electron transfer. Polymeric 2D material, graphitic carbon nitride also shows similar sensing properties upon exfoliation. Kesavan et al. exfoliated graphitic carbon nitride using ultrasonication technique and demonstrated the flutamide (FLT) sensing properties. With the help of impedance spectroscopic studies, they have shown that active sites and conductivity are increased as a result of exfoliation. Along with this, the affinity of FLT and nitrogen on the graphitic carbon nitride played an important role in improving the sensing properties [12].

Irrespective of the layered material, exfoliation is observed to have a significant influence on the sensing properties. Exfoliation results in exposing active sites and the reduction in thickness resulting in better absorption of the analyte molecules and better electron transfer characteristics. Apart from this, the method of exfoliation induces different types of defects on the 2D crystal, the electron density on these defects such as edges and pores have an impact on the electrocatalysis of the analyte molecule. Carefully altering the method of exfoliation, sensing capabilities of the materials could be extended.

10.3 WATER SPLITTING AND FUEL CELLS

Water is an abundant source of energy and splitting water in a most economic route is a serious research concern in recent years for the production of hydrogen and oxygen. Hydrogen is considered the most advantageous renewable source of energy and the availability of oxygen is critical for the treatment of patients affected with COVID 19. Oxygen is also important for the complete combustion of any fuel, including hydrogen. The commercial electrocatalysts containing noble metals are currently used in fuel cells as hydrogen evolution reaction (HER), oxygen evolution reaction (OER), and oxygen reduction reaction (ORR) catalysts. The involvement of noble metals in crucial energy-related applications such as a fuel cell increase the installation and operation cost tremendously. Recently, several non-noble metal electrocatalysts are introduced as a replacement for noble metals and their derivatives. Several 2D layered nanosheets prepared by intercalation/exfoliation are subjected to HER and OER/ORR. Many are identified as potential replacements for noble metals in their respective applications. A list of widely studied exfoliated 2D materials as electrocatalysts are discussed in this session.

10.3.1 Hydrogen Evolution Reaction (HER)

The evolution of hydrogen by electrochemical water splitting can be a feasible way of storing hydrogen for energy-related applications, especially for fuel cells. Over the years, noble metals are broadly used as an efficient catalyst for HERs. However, the high cost of noble metals limits their extensive use as a catalyst at a large scale. To overcome the high cost of noble metal catalysts, electroactive materials that are available in abundance are proposed as catalysts. However, the major challenges of most non-noble materials used in HER are (1) the low efficiency, well below the thermodynamic limits of the water-splitting reaction and (2) the short lifetime [13]. Materials containing transitions metals are very active for HER. Though HER can be performed either in an acid $\left(2H^+ + 2e^- \leftrightarrow H_2\right)$ or basic $\left(2H_2O + 2e^- \leftrightarrow H_2 + 2OH^-\right)$ medium, a basic medium is commonly preferred due to the short-term stability of many materials in the acid medium. Similarly, due to stability issues, pure metals are avoided for HER reactions. To improve the performance of electroactive materials par to the noble metals several strategies are adopted. The suitability of a nanostructured material as an electrocatalyst depends on the surface area, presence of defects such as oxygen vacancies, availability of active sites on the surface, and dopants. The surface area plays an important role in HER since HER is a surface-active reaction.

Materials with the layered structure are identified as a suitable candidate for the HER since the layered materials are often characterized by the presence of multivalent transition metals in their crystal structure and the synergic interaction of these elements can augment the catalysis by offering many active sites for catalyzing the reaction. Interestingly, the conductive flexible 2D nanosheets enable the easy access of the electron from the catalyst substrate to the surface through intimate contact. As a result, the interfacial electron transfer resistance can be reduced and electrons can circulate through the external circuit efficiently [14]. The most active sites of exfoliated 2D materials for HER are located along the edges of the layers, but its performance is currently limited by the density and reactivity of active sites. The unprecedented HER activity of the layered materials is observed when they are exfoliated by intercalating a charged ion such as Li and Na, and thereby surface area is increased enormously in addition to the increased electrical conductivity. The overall HER activity is determined by how well hydrogen atoms can be adsorbed on the catalyst surface [14].

Among the layered materials, the introduction of exfoliated TMDs is a breakthrough in the history of non-noble metal catalysts for HER. Chemically exfoliated layers of dichalcogenides such as MoS_2, WS_2, CoS_2, VS_2, and NiS_2 are extensively studied as a promising electroactive HER catalyst. The above materials exhibit a low overpotential in the range of 100–250 mV vs reversible hydrogen electrode in an acidic medium. Overpotential is the measure of the efficiency of a material for a water-splitting reaction and it represents the loss of the applied voltage. The overpotential of platinum/carbon commercial electrodes are ~30–50 mV. The layered materials without exfoliation or intercalation are often inactive as in the case of MoS_2. The ultra-thinning and 2D nanosheet formation create an abundance of HER active sites at the edges [15]. Moreover, the planar mobility of electrons along the 2D layer guarantees rapid electron transfer from the substrate to active sites. The exfoliated transition metal selenides and tellurides are also reported as electroactive materials for HERs.

For instance, exfoliated WSe_2, $MoSe_2$, $MoS_{2(1-x)}Se_{2x}$, $MoTe_2$, WTe_2, $MoSe_2/WSe_2$, VSe_2, etc. 2D nanosheets exhibited a superior performance than the bulk counterparts. Doping noble metals such as Pt and Ru to the 2D chalcogenides can increase the catalytic activity tremendously. $MoSe_2$ is an n-type semiconductor, converting $MoSe_2$ to a p-type semiconductor by Nb or Ta doping reduces its activity toward HER [16].

MXene (layered metal nitrides and carbides) is a new family of exfoliated materials and potential electrocatalyst for HER, MXene adopts a general formula of $M_{n+1}X_nT_x$ ($n = 1–3$), where M is a transition metal such as Mo, V, or Ti, X is C and/or N, and Tx represents surface functional groups such as H or OH. Despite the high surface area, MXenes are characterized by excellent hydrophilicity and conductivity. Interestingly, the active HER sites for MXene are located on the O^* basal plane, which makes them ideal for HER [17]. The HER activity of MXene is enhanced by modifying the transition metal, during which the Gibbs free energy for hydrogen adsorption is improved, subsequently, one can obtain a decreased barrier energy for hydrogen production [18]. MXene combined with nanostructured platinum is widely used as the electrocatalyst. $Mo_2TiC_2T_x$, $Ti_3C_2T_x$, $V_4C_3T_x$, $Mo_2TiC_2T_x$, etc. are some representative MXene electrocatalysts for HER.

Layered carbon allotropes such as graphene and its oxide exhibit poor adsorption toward hydrogen; therefore, they are not efficient catalysts for HER. However, these materials are extensively used as supporting materials for electroactive elements and nanostructures. The graphene decorated with electroactive nanostructures of Pt, Ni-Mo-N, Ni, CoP, MoS_2, $ReSe_2$, WS_2, etc. is identified as excellent catalysts for HER in a basic medium. In addition to the large surface area, the high conductivity of the graphene/graphene oxide significantly reduces the interfacial electron transfer resistance between the catalyst support and the active sites, which ultimately improves the efficiency toward HER.

10.3.2 Oxygen Evolution Reaction (OER) and Oxygen Reduction Reaction (ORR)

The electrochemical generation of oxygen through water splitting is critical in metal-air batteries and fuel cells. The electrochemical OER ($2H_2O \rightarrow O_2 + 4H^+ + 4e^-$) and ORR ($O_2 + 4H^+ + 4e^- \rightarrow 2H_2O$) are four-electron transfer reactions. Due to the complicated multi-electron transfer steps, the ORR/OER suffers from sluggish kinetics. Similar to HER, noble metals and their derivatives exhibit low overpotential for both ORR (e.g., Pt) and OER (e.g., IrO_2 and RuO_2) applications. 2D nanolayers are unique due to a large number of surface atoms as compared to the internal atoms, which makes them highly electroactive for a variety of applications. Exfoliated 2D materials like graphene and graphene oxide, inorganic monolayer materials such as metal oxides, TMDs, LDHs, MXenes, diatomic hexagonal boron nitride, and black phosphorous (BP or phosphorene) are studied as potential candidates for OER and ORR applications. In addition to the planar strength, exfoliated 2D materials are flexible with an atomic or few-layer thickness. Interestingly, the most single or few layers of graphene, carbon nanosheets (CNS), TMDs, LDHs, and MXenes are exfoliated from their bulk, and these are the most extensively studied 2D materials for OER application.

To overcome the scarcity of OER electrocatalysts for acid medium the transition metal dichalcogenides (TMD) are proposed. The exfoliated 2D nanosheets of MoS_2, TaS_2, WS_2, $MoSe_2$, etc. either in 1T and 2H polymorphic forms are the common electroactive catalysts for OER. The performance of the above materials for OER is par to stable IrO_2. Liquid phase and ion intercalation are the most common routes for the exfoliation of TMDs nanosheets from the bulk by overcoming the weak van der Waals interaction among layers. The step-by-step exfoliation of bulk TMDs using Isopropyl alcohol and the preparation of electrodes using exfoliated nanolayers are shown in Figure 10.3. Alike HER, the dominant active sites of TMDs for OER are on the edges rather than the surface [19]. The dichalcogenides of noble metals such as Rhenium-, Ruthenium-, and Iridium- exhibit exceptional activity toward OER and ORR.

Unlike in the HER, MXenes themselves are not directly active for ORR or OER electrocatalysis; however, they serve as excellent supports for various electroactive materials. MXenes are better catalyst support for Pt nanoparticles or Pt/Pd atoms than carbon as in the commercial Pt/C electrode for OER due to the strong interaction between Pt and the respective MXene layers. Likewise, other electroactive materials such as metal-organic frameworks, carbon nitride, LDHs, oxides, borate, sulfides, and metals bound to the surface of MXenes also exhibited superior OER activity par to the commercial noble metal catalysts. Hybrid TMD–MXene-like materials are recently introduced as OER catalysts. The heterostructure of the above hybrids allows the synergistic interactions between TMDs and MXenes and one can achieve a significant improvement in the OER activity.

Carbon allotropes themselves are not active for OER or ORR, though when doped with heteroatoms (B, S, N, P, F, and O) or transition metals (Ni, Co, Fe, etc.), they become excellent ORR and OER catalysts. The conductivity of graphene, 2D porous

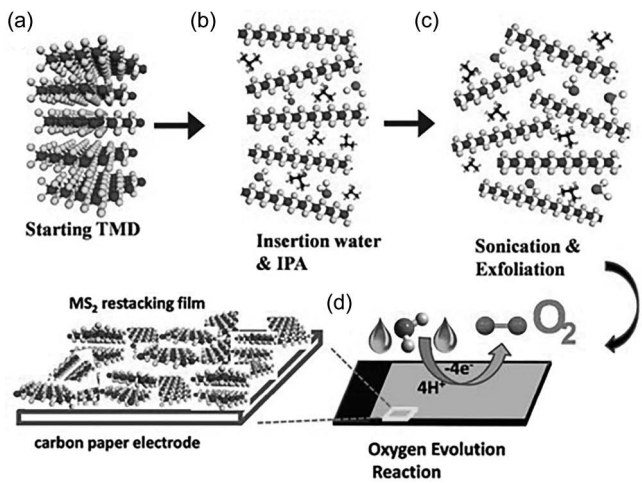


FIGURE 10.3 Schematic representation of step-by-step electrode fabrication process using exfoliated TMDs. (a) Starting TMD, (b) Insertion water and IPA, (c) Sonication and exfoliations, and (d) application for OER (Wu et al. 2016). Reprinted with permission from © 2016 John Wiley and Sons.

carbon, and graphitic carbon nitride (g-C_3N_4) layers can significantly reduce the interfacial resistance between the electroactive materials or the active sites and the current-carrying substrate. Additionally, as discussed in the case MXenes, the exfoliated 2D carbon layers are commonly used as a support for nanosized or atomic catalytic materials. MoS_2, Fe_3O_4, FeP, Ni_2P, CoP_2, CoO_x, NiO, etc. are some representative nanoparticles grown on 2D carbon materials for OER. Nevertheless, the long-term stability of carbon-based electrocatalysts is inferior to MXenes. Both MXenes and 2D carbon allotropes are mostly sought for OER and ORR in a basic medium.

Among the OER catalysts, layered double hydroxides (LDHs) are extensively studied as a potential replacement for noble metal catalysts due to their compositional and structural flexibility in addition to the simple preparation routes. Often LDHs adopt a formula either $M_x^{2+}M_{1-x}^{3+}(OH)_2\left(A^{n-}\right)_{\frac{x}{n}}.\ yH_2O$ or $M_x^{1+}M_{1-x}^{4+}(OH)_2\left(A^{n-}\right)_{\frac{x}{n}}.\ yH_2O$; where M is a metal and A is the intercalating anion. In LDHs, every single layer is composed of edge-sharing octahedral MO_6 moieties (M stands for metal) as shown in Figure 10.4. The color code used in the figure are: purple for metals, red for oxygen, and grey for inter-layer anions and water molecules. If d_1 is the inter-layer distance before intercalation, the inter-layer distance increases after intercalation to d_2 and $d_2 > d_1$. One can observe the change in interlayer spacing under an electron microscope and the subsequent change in the crystal structure from X-ray diffraction. The transition metal oxides (TMOs) with *d*-orbitals can effectively bind oxygen species on its surface, which is an essential requirement for OER/ORR catalyst. The substitution of elements in M^{2+} and M^{3+} sites can fine-tune the electronic as well as the catalytic properties of LDHs. Exfoliated LDHs formed by a combination of the transition metals, Ni-Co, Ni-Fe, Co-Fe, Co-Co, Ni-Mn, Co-Mn, etc. are some representative low overpotential electrocatalysts for OER in a basic medium among the non-noble metal catalysts.

Exfoliated layered perovskite with the general formula ABO_3 (A and B can be occupied by a large number of elements in the periodic table) and delafossite with the general formula AMO_2 is also studied as potential OER catalysts [20]. The above oxides with transition metals such as Co, Ni, and Fe at one of the sites are excellent OER catalysts. Such oxides are stable than the carbon-containing catalysts under oxidative environments and offer a competitive catalytic property comparable to noble metals.

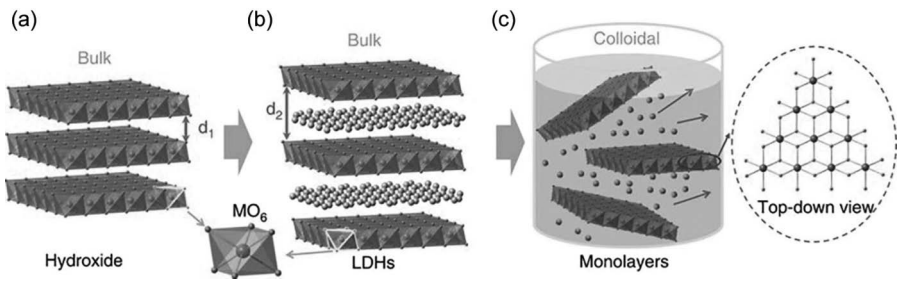


FIGURE 10.4 (a) Structure of layered hydroxides, (b) LDHs intercalated with a layer of anions and water molecules, and (c) exfoliated LDH monolayers in a colloidal solution (Song and Hu 2014). Reprinted with permission from © 2014 Springer Nature.

10.4 SUPERCAPACITORS

Supercapacitors bridge the gap between rechargeable batteries and conventional capacitors. But one of the major restrictions of supercapacitors is their lower energy density than the rechargeable batteries. There are several reported attempts to improve and enhance the energy density of supercapacitors. Supercapacitors mainly consist of electrodes, electrolytes, current collectors, sealants, and separators. The selection and design of the electrode materials have a major role in the overall performance of a supercapacitor as it determines the ionic conductivity, surface area, and chemical and thermal stability [21].

Supercapacitors are categorized mainly into two, based on their charge storage mechanism, one is electric double-layer (EDLC) or faradaic capacitor where energy is stored via non-Faradaic electrostatic interaction and the other one is pseudocapacitor where the energy storage is accomplished through Faradaic redox charge transfer reactions [22]. When 2D layered nanomaterials are used as electrodes in both Faradaic and non-Faradaic storage systems, the charge is mainly stored at the basal plane of the layered nanosheet, i.e., with the larger planar area. Additionally, the presence of active edge sites and the weak van der Waals gap between the nanosheet layers of 2D nanomaterials offer enhanced and suitable electrochemical performance in supercapacitors. Here in this section, the most commonly used exfoliated 2D nanosheets of both carbon-based and non-carbon-based are discussed in detail.

Graphene is one of the most common 2D layered carbon sheets with a hexagonal lattice structure, widely investigated for supercapacitor applications. The kinetics of an electrode material mainly depends on the transportation and diffusion of electrolyte ions. Due to the lack of enough edge planes and surface charges, monolayer graphene is considered one of the most chemically and electrochemically inert materials [23]. During the charge storage process, graphene acts as a superior active material as the electrolyte ions like Na^+, K^+, etc., can be stored electrostatically on the electrode. But the agglomeration of graphene nanosheets due to the strong van der Waals interaction limits the full utilization of graphene surface for ion adsorption. The agglomerated structure extremely limits the direct access to the charge-storage surfaces, which finally leads to the increase in ionic resistance at the electrode [24]. Higher agglomeration, hydrophobicity, and the random orientation of graphene nanosheets restrict the availability of ions on the active surface. Thus, the morphology of the electrode materials plays a vital role in the charge storage mechanism of supercapacitors.

Stoller et al. developed chemically modified graphene (CMG) electrodes with good electrical conductivity and a specific surface area of 705 $m^2 g^{-1}$, by chemical functionalization of monolayer graphene. The CMG electrode materials exhibited a specific capacitance of 135 F g^{-1} in aqueous electrolyte (5.5 M KOH) and 99 F g^{-1} in the organic electrolyte [25]. Most reported graphene-derived electrode materials exhibited lower specific surface area than their theoretical value (2,630 $m^2 g^{-1}$). But the Ruoff group reported KOH-activated thermally exfoliated graphene oxide and microwave exfoliated graphene oxide (MEGO) electrode material, which exhibited an ultrahigh specific surface area value of 3,100 $m^2 g^{-1}$, a high electrical conductivity (~500 $S.m^{-1}$), high content of sp^2-bonded carbon, and low hydrogen content. The KOH-activated MEGO electrode exhibited a notable high energy density (~70 Wh kg^{-1})

and power density (~250 kW kg^{-1}) at a current density of 5.7 A g^{-1} [26]. El-Kady et al. fabricated a graphene-based supercapacitor via laser irradiation of a graphene oxide film coated on a flexible substrate mounted in a LightScribe DVD optical drive. The graphene oxide sheets stacked in the film were reduced and exfoliated simultaneously upon laser irradiation and this structure restricts the agglomeration of graphene sheets and also the open pores in them facilitate the easy accessibility of electrolyte on the electrode surface. The resultant laser-scribed graphene sheets exhibited a high specific surface area of 1,520 $m^2 g^{-1}$, good mechanical flexibility, and high electrical conductivity (1,738 $S.m^{-1}$) [27]. Miller and his group fabricated supercapacitor electrodes using radio frequency plasma-enhanced chemical vapor deposition in which vertically oriented graphene nanosheets were deposited on a heated Ni-substrate. They showed a specific surface area of ~ 1,100 $m^2 g^{-1}$ and effective filtering of 120 Hz current with a resistance-capacitance time constant value less than 0.2 ms. With the exposed edge planes the vertically aligned graphene nanosheets showed enhanced charge storage as compared to the flat graphene nanosheets [28]. The exceptional properties and promising application of graphene in energy storage devices have triggered a remarkable interest in exploring other non-carbon 2D layered nanostructures with versatile properties.

Non-carbon-based 2D layered nanomaterials have been considered as a potential candidate for supercapacitor electrodes owing to their unique physical and chemical properties such as high electronic conductivity, tunable surface chemistry, more surface-active sites, dual non-faradaic and faradaic electrochemical performances, and larger mechanical strength. 2D non-CNSs include TMDs (MoS_2, WS_2, TiS_2, ZrS_2, $MoSe_2$, WSe_2, etc.), layered metal-oxides, hexagonal boron nitride (h-BN), LDHs, graphitic carbon nitride (g-C_3N_4), and MXenes (Ti_3C_2, V_2C, Ti_2AlC, TiAlC, Ti_3CN) [29]. Among TMDs, 2D MoS_2 nanosheets are a potential supercapacitor electrode material that exhibits large electrical double layer capacitance (EDLC) owing to their stacked sheet-like structure, and large pseudocapacitance due to the different Mo oxidation states (+2 to +6). Tour and his co-workers developed vertically aligned/edge-oriented MoS_2 nanosheets that offer a high capacitive property with more van der Waals gaps and rendered reactive dangling bonds sites for the electrolyte ions. Areal Capacitance of 12.5 mF cm^{-2} was obtained for sponge-like vertically aligned MoS_2 electrodes [30]. Layered 2D TMOs exhibit exceptionally high surface area and high conductivity as they are capable of holding charged ions on their surface without intermixing. Supercapacitors based on layered TMOs feature superior cyclic stability, high energy density, and high discharge currents. Commonly used 2D layered TMOs include MnO_2, NiO, Co_3O_4, and RuO_2. MnO_2 possesses low conductivity and thus they require a conductive matrix of graphene or metal foam. Peng et al. fabricated a supercapacitor electrode integrating 2D graphene and 2D MnO_2 into a planar capacitor design that was highly flexible [31].

2D LDH sheets are a class of multi-metal clay materials that consist of metal cations brucite layers octahedrally surrounded by hydroxyls forming $M^{2+}(OH)_6/M^{3+}/M^{4+}(OH)_6$ octahedra. Their high redox activities can be attributed to their unique properties like cations, easy tenability in their host layers and they are capable of exchanging anions without disturbing the structure. In NiAl-LDH, its electrochemical

property is due to a mixed mechanism comprising of 'electron hopping' along with the layers of LDH and the migration of protons from the host layer to the solution [32]. MXenes have become a widely accepted supercapacitor electrode material with their impressive electrochemical properties due to their unique 2D structure and well-defined geometry. MXenes are one of the fast-growing materials among 2D materials, which include metal carbides, nitrides, and carbonitrides. One of the promising features of MXene is the exceptionally large interlayer spacing, which helps in the de/intercalation of ions like Na^+, Li^+, etc. Mainly hydrogen bonding and van der Waals bonding interactions act between the MXene layers. To produce MXene single flake suspensions, water, cations, tetrabutylammonium hydroxide (TBAOH), dimethylsulfoxide (DMSO), etc. are intercalated into the MXene interlayer spacing followed by the sonication process. In the H_2SO_4 electrolyte, $Ti_3C_2T_x$ shows a high volumetric capacitance of ~1,500 F cm^{-3} (380 F g^{-1}), and the conductive, transparent $Ti_3C_2T_x$ films are used to fabricate solid-state transparent supercapacitors [33].

10.5 LITHIUM-ION BATTERY

Lithium-ion batteries (LIBs) are the answer to many of the energy storage-related challenges. LIBs become an essential part of everyday life. LIBs work by the rocking chair mechanism wherein the lithium ions are moved between the anodes and cathodes. The electrodes play an important role in storing the lithium ions by the intercalation and deintercalation reactions. Historically, layered materials have played an important role in the development of LIBs by allowing the layered structures of the electrodes like graphite to intercalate lithium ions. Currently, LIBs use a wide variety of electrodes having mechanisms such as insertion, alloying, and conversion reactions [34]. Electrodes with higher rate capability, higher charge capacity, and (for cathodes) sufficiently high voltage can improve the energy and power densities of Li batteries and make them smaller and cheaper. The fast-paced life around the globe is forcing researchers to focus on materials that can be charged faster and hold more energy per volume and weight. Layered materials are often helpful in achieving faster lithium-ion diffusion and have a higher capacitive contribution. Owing to compelling electrochemical and mechanical properties, exfoliated 2D nanomaterials have been propelled to the forefront in investigations of electrode materials in recent years.

Exfoliated 2D nanomaterials are exceedingly desirable as anodes and cathodes. As anodes, the famous candidates are graphene and graphene-based composite materials, including carbon nanotubes/graphene, nonmetal/graphene, TMOs/graphene, sulfide/graphene, and salts/graphene. As cathodes, exfoliated 2D nanomaterials have remarkable electron transport velocity, high theoretical capacity, and excellent structural stability. The exfoliation of bulk material and Li^+ insertion was represented in Figure 10.5, which shows easier paths for lithium-ion storage.

Graphite is the most traditionally used anode in LIBs, which is a layered material. Expansion and exfoliation of the graphite are well reported by various researchers. Graphite as such shows a theoretical capacity of 372 mAh g^{-1}. Due to good electrical conductivity, high surface area, and greater mechanical flexibility, graphite exfoliation has attracted the most attention for fabricating high-performance electrode material for LIB. Lithium may bond both graphene sheet sides as well as edges and

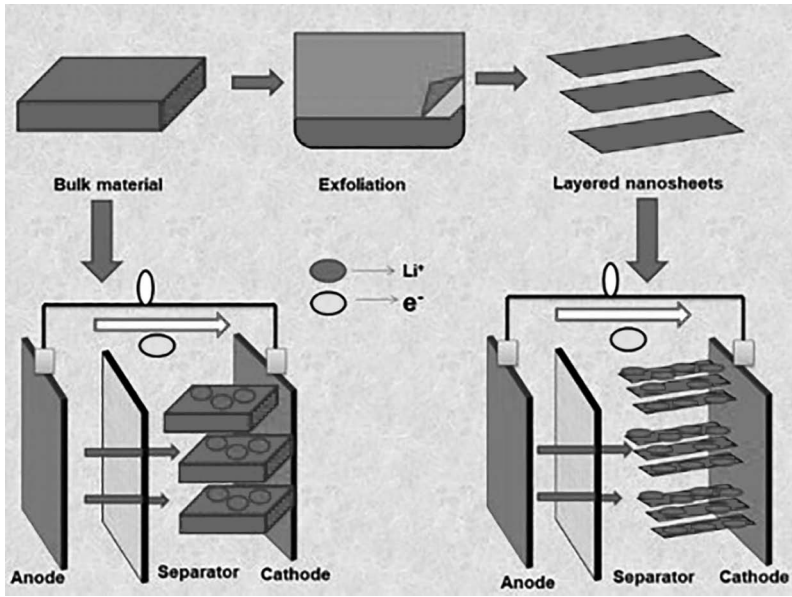


FIGURE 10.5 Sketch of the exfoliated layered material as a cathode for Li^+ insertion in LIBs.

covalent sites. Recent studies demonstrated that the small lateral sizes of narrow graphene nano-ribbons can accommodate Li^+ ions at the edges sites more efficiently than basal sites, thus leading to maximum Li-storage in the form of Li_4C_6. The probable defects formed during the exfoliation process become an advantage in such cases. Apart from this, graphene nanosheets are widely used to make composites with other electrode materials. In materials like silicon, graphene sheets are also used to give cushioning effect to accommodate the high volume change during the lithium uptake.

Exfoliated carbons are trustable electrodes for lithium battery electrodes but lack high capacity, which restricts the overall capacity of the batteries. Exfoliated 2D group V nano-crystals have a greater theoretical capacity than graphite. Exfoliation of these metallic electrodes is challenging because of the stability issues. Among them, layered 2D antimony has the potential as electrode material for LIBs, owing to their large interlayer distance in their layered structure, high capacity, long mean free path, and environmental friendliness. The theoretical capacity of antimony is moderate therefore other 2D materials are also explored as LIB electrodes. The layered transition metal oxides (LTMOs) require a special mention in LIBs. The exceptional feature of these materials is the presence of an interlayer region that serves as the host for ion intercalation. The extensive interlayer spacing and weak interlayer bonding of LTMOs permit the intercalation of an enormous variety of guest species, like cations, polymers, and anions. LTMO has excellent electronic and ionic conductivity, the attainability of interlayer sites for the intercalation of cations from the electrolyte, and the ability to undergo redox reaction property for high energy density LIB. Several mechanisms are possible when LTMO is in contact with an electrolyte like intercalation, conversion, double layer capacitance, conversion, and pseudocapacitance [35].

2D TMDs consist of greater specific capacity and larger interlayer spacing, which permit a quick Li^+ insertion/extraction process without persuading noteworthy volume changes [36]. Exfoliated layers of chalcogenides such as MoS_2, $NbSe_2$, WS_2, $MoSe_2$, $TaSe_2$, and $MoTe_2$ nanosheets are widely used for the LIB. Among them, MoS_2 is an exciting electrode material for LIBs due to its high theoretical capacity. MoS_2 nanolayers allow intercalation of Li^+ ions into the structure without noteworthy volume change and charging and discharging prevent the disintegration of active material. Based on the reaction $MoS_2 + 4Li^+ + 4e^- \leftrightarrow 2Li_2S + Mo$, the electrochemical reaction of Li with MoS_2 involves 4 moles of Li per mole of MoS_2. The main concern of MoS_2 layered nanomaterial is low electronic conductivity and poor cyclic stability [37].

Another class of materials that is gaining recent attention is MXenes, which possess 2D layered structure. The main advantage of MXene as electrode material for the energy storage device is the separation between MXene layers that can be controlled systematically. MXenes usage as anode for LIBs was first reported by Naguib et al. [38]. The MXenes prepared by Naguib showed improved surface area by ~10-fold as compared with graphene since MXenes exhibit improved specific capacity. Layered morphology of the electrodes always had a positive impact on LIBs by facilitating the rocking chair mechanism. Fast charging and higher capacities are repeatedly reported as a result of exfoliation. Structural changes during the exfoliation are usually acting in favor of the intercalation of more lithium ions to the electrodes. Therefore, exfoliated 2D materials are going to have a large impact on the future development of LIBs.

10.6 CONCLUSIONS

Exfoliated 2D nanosheets have gained considerable attention from the research community in recent years. The development of various 2D nanosheets of different origins allows the researchers to resolve numerous bottlenecks associated with many electrochemical devices, especially in sensors, fuels cells, supercapacitors, and batteries. Though exfoliation is a top-down approach, it can produce reasonably good quality nanosheets in large quantities, which is essential for device fabrication at a large scale. Interestingly the defects generated during exfoliation favor electrochemical activity than the ones prepared by chemical vapor deposition with fewer defects. The exfoliated 2D materials are expected to play an important role in the further advancements in electrochemical devices in the coming years.

REFERENCES

1. Guo B., Xiao Q., Wang S., Zhang H. (2019) 2D layered materials: Synthesis, nonlinear optical properties, and device applications. *Laser Photon Rev* 13:1800327.
2. Alzakia F.I., Tan S.C. (2021) Liquid-exfoliated 2D materials for optoelectronic applications. *Adv Sci* 8:2003864.
3. Zhou Y., Pondick J.V., Silva J.L., Woods J.M., Hynek D.J., Matthews G., Shen X., Feng Q., Liu W., Lu Z., Liang Z., Brena B., Cai Z., Wu M., Jiao L., Hu S., Wang H., Araujo C.M., Cha J.J. (2019) Unveiling the interfacial effects for enhanced hydrogen evolution reaction on MoS_2/WTe_2 hybrid structures. *Small* 15:1900078.
4. Anasori B., Lukatskaya M.R., Gogotsi Y. (2017) 2D metal carbides and nitrides (MXenes) for energy storage. *Nat Rev Mater* 22(2):1–17.

5. Kumar S., Pavelyev V., Mishra P., Tripathi N., Sharma P., Calle F. (2020) A review on 2D transition metal di-chalcogenides and metal oxide nanostructures based NO_2 gas sensors. *Mater Sci Semicond Process* 107:104865.
6. Huo C., Yan Z., Song X., Zeng H. (2015) 2D materials via liquid exfoliation: A review on fabrication and applications. *Sci Bull* 60:1994–2008.
7. Ndlovu T., Arotiba O.A., Sampath S., Krause R.W., Mamba B.B. (2012) An exfoliated graphite-based bisphenol a electrochemical sensor. *Sensors* 12:11601–11611.
8. Sreejesh M., Huang N.M., Nagaraja H.S. (2015) Solar exfoliated graphene and its application in supercapacitors and electrochemical H_2O_2 sensing. *Electrochim Acta* 160:94–99.
9. Aswathi R., Sandhya K.Y. (2018) Ultrasensitive and selective electrochemical sensing of Hg(II) ions in normal and sea water using solvent exfoliated MoS_2: Affinity matters. *J Mater Chem A* 6:14602–14613.
10. Moolayadukkam S., Thomas S., Sahoo R.C., Lee C.H., Lee S.U., Matte H.S.S.R. (2020) Role of transition metals in layered double hydroxides for differentiating the oxygen evolution and nonenzymatic glucose sensing. *ACS Appl Mater Interfaces* 12:6193–6204.
11. Sahoo R.C., Moolayadukkam S., Thomas S., Asle Zaeem M., Matte H.S.S.R. (2021) Solution processed Ni_2Co layered double hydroxides for high performance electrochemical sensors. *Appl Surf Sci* 541:148270.
12. Kesavan G., Chen S.M. (2020) Sonochemically exfoliated graphitic-carbon nitride for the electrochemical detection of flutamide in environmental samples. *Diam Relat Mater* 108:107975.
13. Strmcnik D., Lopes P.P., Genorio B., Stamenkovic V.R., Markovic N.M. (2016) Design principles for hydrogen evolution reaction catalyst materials. *Nano Energy* 29:29–36.
14. Di J., Yan C., Handoko A.D., Seh Z.W., Li H., Liu Z. (2018) Ultrathin two-dimensional materials for photo- and electrocatalytic hydrogen evolution. *Mater Today* 21:749–770.
15. Gao M.-R., Chan M.K.Y., Sun Y. (2015) Edge-terminated molybdenum disulfide with a 9.4-Åinterlayer spacing for electrochemical hydrogen production. *Nat Commun* 6:1–8.
16. Chua X.J., Luxa J., Eng A.Y.S., Tan S.M., Sofer Z., Pumera M. (2016) Negative electrocatalytic effects of p-doping niobium and tantalum on MoS_2 and WS_2 for the hydrogen evolution reaction and oxygen reduction reaction. *ACS Catal* 6:5724–5734.
17. Handoko A.D., Fredrickson K.D., Anasori B., Convey K.W., Johnson L.R., Gogotsi Y., Vojvodic A., Seh Z.W. (2017) Tuning the basal plane functionalization of two-dimensional metal carbides (MXenes) to control hydrogen evolution activity. *ACS Appl Energy Mater* 1:173–180.
18. Li P., Zhu J., Handoko A.D., Zhang R., Wang H., Legut D., Wen X., Fu Z., Seh Z.W., Zhang Q. (2018) High-throughput theoretical optimization of the hydrogen evolution reaction on MXenes by transition metal modification. *J Mater Chem A* 6:4271–4278.
19. Hemanth N.R., Kim T., Kim B., Jadhav A.H., Lee K., Chaudhari N.K. (2021) Transition metal dichalcogenide-decorated MXenes: Promising hybrid electrodes for energy storage and conversion applications. *Mater Chem Front* 5:3298–3321.
20. George G., Ede S.R., Luo Z. (Professor of materials science) (2020) *Fundamentals of Perovskite Oxides: Synthesis, Structure, Properties and Applications*. CRC Press, Boca Raton, FL.
21. Forouzandeh P., Pillai S.C. (2021) Two-dimensional (2D) electrode materials for supercapacitors. *Mater Today Proc* 41:498–505.
22. Gholamvand Z., McAteer D., Harvey A., Backes C., Coleman J.N. (2016) Electrochemical applications of two-dimensional nanosheets: The effect of nanosheet length and thickness. *Chem Mater* 28:2641–2651.
23. Huang X., Zeng Z., Fan Z., Liu J., Zhang H. (2012) Graphene-based electrodes. *Adv Mater* 24:5979–6004.

24. Dong Y., Wu Z.S., Ren W., Cheng H.M., Bao X. (2017) Graphene: A promising 2D material for electrochemical energy storage. *Sci Bull* 62:724–740.
25. Stoller M.D., Park S., Zhu Y., An J., Ruoff R.S. (2008) Graphene-based ultracapacitors. *Nano Lett* 8:3498–3502.
26. Zhu Y., Murali S., Stoller M.D., Ganesh K.J., Cai W., Ferreira P.J., Pirkle A., Wallace R.M., Cychosz K.A., Thommes M., Su D., Stach E.A., Ruoff R.S. (2011) Carbon-based supercapacitors produced by activation of graphene. *Science* 332:1537–1541.
27. El-Kady M.F., Strong V., Dubin S., Kaner R.B. (2012) Laser scribing of high-performance and flexible graphene-based electrochemical capacitors. *Science* 335:1326–1330.
28. Miller J.R., Outlaw R.A., Holloway B.C. (2010) Graphene double-layer capacitor with ac line-filtering performance. *Science* 329:1637–1639.
29. Yang Y., Hou H., Zou G., Shi W., Shuai H., Li J., Ji X. (2018) Electrochemical exfoliation of graphene-like two-dimensional nanomaterials. *Nanoscale* 11:16–33.
30. Yang Y., Fei H., Ruan G., Xiang C., Tour J.M. (2014) Edge-oriented MoS_2 nanoporous films as flexible electrodes for hydrogen evolution reactions and supercapacitor devices. *Adv Mater 2*6:8163–8168.
31. Peng L., Peng X., Liu B., Wu C., Xie Y., Yu G. (2013) Ultrathin two-dimensional MnO_2/Graphene hybrid nanostructures for high-performance, flexible planar supercapacitors. *Nano Lett* 13:2151–2157.
32. Li X., Du D., Zhang Y., Xing W., Xue Q., Yan Z. (2017) Layered double hydroxides toward high-performance supercapacitors. *J Mater Chem A* 5:15460–15485.
33. Hu M., Zhang H., Hu T., Fan B., Wang X., Li Z. (2020) Emerging 2D MXenes for supercapacitors: Status, challenges and prospects. *Chem Soc Rev* 49:6666–6693.
34. Pender J.P., Jha G., Youn D.H., Ziegler J.M., Andoni I., Choi E.J., Heller A., Dunn B.S., Weiss P.S., Penner R.M., Mullins C.B. (2020) Electrode degradation in lithium-ion batteries. *ACS Nano* 14:1243–1295.
35. Augustyn V. (2017) Tuning the interlayer of transition metal oxides for electrochemical energy storage. *J Mater Res* 32:2–15.
36. Wu S., Du Y., Sun S. (2017) Transition metal dichalcogenide based nanomaterials for rechargeable batteries. *Chem Eng J* 307:189–207.
37. Choi W., Choudhary N., Han G.H., Park J., Akinwande D., Lee Y.H. (2017) Recent development of two-dimensional transition metal dichalcogenides and their applications. *Mater Today* 20:116–130.
38. Naguib M., Mochalin V.N., Barsoum M.W., Gogotsi Y. (2014) 25th anniversary article: MXenes: A new family of two-dimensional materials. *Adv Mater* 26:992–1005.

2021 National Conference on Sustainable Practices in Civil Engineering

Bio-reactor Landfill for Sustainable Waste Management – A Review

Akhila M
Dept. of Civil Engineering
SCMS School of Engineering and Technology
Ernakulam, India
akhila144@gmail.com

Anjali A M
Dept. of Civil Engineering
SCMS School of Engineering and Technology
Ernakulam, India
am.anjalianju@gmail.com

***Abstract* - To improve personal satisfaction in any country, the strategies for strong waste management should be reinforced. In India, the concept of engineered landfilling is not fully utilized. On the off chance that enough land is usable, it is viewed as a savvy practice. Aside from certain progressions, for example, reusing and source moderation methodologies, it has been found that garbage removal in landfills will stay an unavoidable piece of the strong waste administration framework. The bioreactor landfill concept changes the purpose of landfilling from storage to treatment of waste. The working hypothesis is that they encourage and speed up the natural exploitation of waste by safeguarding ideal dampness content inside the cells where the squanders are handled. The distribution of leachate assists with controlling dampness and microorganisms help to settle natural waste. The development of Bioreactor landfills can give natural and monetary advantages, and it is a promising strong waste administration framework for a thickly populated and emerging nation like India. This paper examines the possibility of a Bioreactor landfill for waste handling in the Indian context. The main features, types, operations, advantages, disadvantages and differences to the conventional landfills are discussed in detail.**

Keywords—bioreactor landfill, waste disposal, sustainability

I. INTRODUCTION

Attributable to different sources of strong waste with quick development in the populace worldwide, maintainable metropolitan strong waste administration has become a necessity. The age of MSW has become an inexorably significant worldwide issue throughout the most recent decade. The expanded age of strong waste has provoked the execution of coordinated MSW the board, which incorporates reusing, fertilizing the soil, incineration and landfilling. About 80% to 90% of metropolitan waste is discarded in landfills without proper administration strategies or open copying, as indicated by gauges prompting air, water, soil contamination. Natural substances and actual cycles in landfill conditions encourage the biodegradation of natural squanders in MSW. Natural boundaries, like landfill liners and covers, are regularly utilized in ordinary landfills to keep dampness out, which is essential for waste biodegradation. Therefore, wastes are caught in a "dry burial place" and stay unharmed for extensive stretches going from 30 to 200 years, possibly outliving the landfill obstructions and covers. Liner disappointment in customary dry landfills is a chance, later on, representing a critical danger of groundwater and surface water pollution. Today, one idea that has got a ton of consideration is the "Bioreactor landfill." Within 5 to 10 years of presenting the bioreactor interaction, a bioreactor landfill is a sterile landfill that utilizes improved microbiological cycles to change over and balance out the promptly and respectably decomposable natural waste constituents. In contrast with what might somehow occur in a landfill, the bioreactor landfill incredibly builds the level of natural waste decay, transformation rates, and cycle adequacy. The expansion of leachate or other fluid revisions, the expansion of sewage muck or different alterations, temperature control, and a "bioreactor landfill" give control and cycle streamlining, mostly through the expansion of leachate or other fluid changes, temperature control, and supplement supplementation. Additionally, the activity of a bioreactor landfill can require the option of air. Various types of "bioreactor landfills, for example, anaerobic bioreactors, oxygen-consuming bioreactors, and vigorous anaerobic bioreactors have been created and worked around the planet dependent on waste biodegradation mechanisms.

This paper means to raise peruse consciousness of the bioreactor landfill as a possibly reasonable waste management tool. It is required to be an essential commitment to future conversations among landfill proprietors and administrators, lawmakers, controllers, preservationists, and the overall population.

II. WASTE MANAGEMENT IN INDIA

It has been found that MSW, which ordinarily contains half biodegradable materials, 20% recyclable materials, and 30% dormant and inorganic materials including sands, rocks, and rock, has enormous energy potential. The metropolitan urban communities and towns of India's different states produce about 0.5 kg of MSW per capita each day. Only 12–14 % of MSW is formally taken care of in India, with the rest going to open unloading and landfill removal choices. As per the Planning Commission Report (2014), around 377 million individuals living in metropolitan territories produce 62 million tons of MSW each year, with 165 million tons each year and 436 million tons each year projected later on. The MSWM rules are set up to decrease the measure of waste that winds up in landfills by reusing likely material and assets from MSW. The various waste management methods for Indian MSW are listed below (Nandan et al., 2017; Pujara et al., 2019)

ISBN: 978-93-5493-715-6