WiFi Data Leakage Detection

Pranav Shrivastava1, Prerna Agarwal2, Rahul3, Monika4

1 Assistant Professor, CSE Department, GLBITM, Greater Noida, India
2 Assistant Professor, CSE Department, JIMSTEC, Greater Noida, India
3 Assistant Professor, CSE Department, DTU, New Delhi, India
4 Research Scholar, DTU, New Delhi, India
pranav.paddy@gmail.com
9582775504

Abstract

The applications that we install on smart phones generates multitude of network traffic patterns, background activities, periodic updates etc. This application data leak side channel information like packet size, transfer timing, volume etc. This information can be used and exploited by an intruder to steal confidential user information. This paper focuses on various threats to the user’s private activities with the increase in commercial interest in tracing publicly broadcasted wireless data. The paper demonstrates mechanisms for inferring the user behavior from encrypted wireless network activity. It also shows how an absolutely inert eavesdropper can detect the information that is being transmitted over the network.

Keywords

WiFi, Mobile-Applications, Confidentiality, Safety, Data Protection, Information Abstraction, Encryption

1. Introduction

1.1. Data Leakage

Involuntary or fortuitous dissemination of confidential or susceptible data to an illegitimate entity is known as data leakage. Whilst data stored in data centers is transmitted in an unauthorized and uncontrolled manner, data leakage occurs. Data leakage can lead to huge losses to the organization and also result in loss of trust of the people. Data leakage is said to have occurred when an unauthorized user access the sensitive data which consists of intellectual property, monetary data, private information such as contact information, credit-card information, & similar confidential information. Data leakage is a very common and important issue these days. The number of incidents and the users affected by it are on a rise. The reason of exposure of confidential data or information might be malevolent objective or an unintentional lapse, but it can gravely damage the organizations’ reputation.

1.2. Scenario and Environment

WiFi data usage and communication is escalating and is now a basic need of an ever-increasing modern society; permeating through homes, business and almost everywhere. Sensitive data may include intellectual property (IP), monetary data, patient data, credit-card information, & the business and the industry specific data. In event of data leakage the company becomes vulnerable and this may put business in a defenseless spot. As the amount of data leakage incidents and their detriment go on to intensify, it instigates severe issues for companies.
With companies recognizing wireless broadcasts as an important source of data for their growth, the business-related awareness in wireless broadcasts has increased ever since making access points more common and popular. Our study concentrates on review of work done with the ‘side-channel’ information on WiFi. In order to show user activity inference, 34 popular and secure applications were selected, and the intended demographics of their users were found out. The next step was to collect the network data when users opened the applications. The usage of a particular application is determined by the network activity [1]. But because of encryption, only limited amount of information is available through side-channels. Histograms were constructed from frame size classification and inter-arrival time characteristics. These histograms detail the metrics distribution over a period of time.

This technique can recognize application which can be helpful in fingerprinting of different activities over the encrypted communication system. Mobile application is an appropriate and a vulnerable target due to their personal ties with other applications, availability in an openly ranked market with comparatively less diversity and the ease of collections. Although the methods shown in this paper use 802.11d WiFi standard, the processes should generalize to other protocols of wireless communications as well excluding those which are by-design intended to withstand this category of scrutiny [1]. Especially supportive of mobile applications, the methods and measurements employed to carry out...
this investigation will moreover be in attendance in long range protocols like 4G LTE network available in cell phones.

However, here we tried to review about how the combination of Direction, Frame size and Inter-arrival timing of the data packet makes user’s personal and insightful information vulnerable. Any passive party within the wireless network range can cause information leakage. The observer here does not attempt to breach the encryptions in place and instead functions devoid of any degree of network access or authorization. Skype traffic was also analyzed to infer user activities. Even when the Skype traffic is combined with different and more confusing traffic simultaneously, the detection ability still remains the same. This in turn makes it remote, passive, undetectable and inexpensive.

A closer look at Fig 1.3 shows a description so as how a mobile device gets connected to an Access Point (AP), a service provided by Internet Service Provider (ISP). The applications running on any device using internet may use the same link to correspond with specific remote internet servers. The content of the application is provided through the information from these servers. One of the main advantages of being dependent on an internet connection is that its centralized architecture reduces the dependency over processing power and storage. These equipments can thus be smaller, cheaper and also offer latest content or backups when connected. Also, internet connection is also exploited to a certain extent by applications that only offer unchanging limited subject matter, whenever accessible. In current 802.11g Wi-Fi network setup, access point offers industry benchmark encryption so that only the users who have access to the network access it.

![Figure 3 Observing encrypted mobile device WiFi traffic.](image)

2. RELATED WORK

Today, Wifi is widespread everywhere around the world. The broadcast nature of wireless networks utilizes different nearby applications to detect receiver’s location and is a familiar phenomenon in various mobile devices. Though encryption technique is used for maintaining the confidentiality of data in wireless communications over wide area, the unbroken encryption can also affect the user’s activities to large extent about which many people are still not aware. However great amount of effort is needed to carry out these kinds of analysis and therefore is not much prevalent.

In order to achieve compatibility, most of the network protocols follow OSI model. OSI model separates the protocols into different layers with respect to their responsibilities. The data at lower layer protocols is encapsulated with the higher ones. The WiFi standard (IEEE 802.11) redefines the Data Link layer and Physical layer of OSI model and has been modified from the wired Ethernet
standard (IEEE 802.3) [3]. To ensure confidentiality of data, WiFi networks must employ an encryption technique in order to prevent data from being read directly by an unauthorized user. The work below has not attempted to discover or abuse defects to breach WiFi encryption.

John et al [1] discusses about the methods used by mobile device applications that can involuntarily broadcast user’s private data via exploiting wireless networks regardless of encryption working perfectly as designed. It is demonstrated how usage of application is capable of coupling to private data through selection of personas. Personal information is assumed to be confidential by the users while using a network that is encrypted. Yet, they have illustrated methods of analyzing an encrypted traffic pattern to permit a distant onlooker to deduce possibly susceptible information inertly and untraceably devoid of network authorization. [4]

Availability of limited side channel data enables remote app detection. However, here we do not have the capability to read encoded WiFi data directly. Histograms that epitomize side-channel information dimensions are used to construct Random Forest classifier. It is capable to precisely identify mobile applications from their generated encrypted traffic. In order to accurately identify the applications this algorithm has an accuracy of ~99% in the training set [5]. Finally, potential applications, methods to minimize such kind of data leaks and efforts required to demonstrate this phenomenon to users is discussed. This paper highlights a privacy vulnerability that is difficult to solve and cannot be minimized without making significant changes to the existing and subsequent generation of wireless communication protocols.

Atkinson et al [26] illustrated a method for inferring user behavior from encrypted wireless network activity. Even without the necessity of breaking any encryption or having any level of network access this mechanism operates successfully. It demonstrates how a completely passive and remote observer can identify when a user is operating Skype and when not. Also illustrated is the identification capability even when Skype’s traffic is combined with incomprehensible concurrent traffic such as Bittorrent. Method demonstrated here confronts the presumptions that secure cryptography means safe and sound information & the approach of mechanisms exploited possibly will facilitate analyzing encrypted data in progressively significant volumes. Based on the difference in the size of the frame and its interarrival time, we were able to distinguish between the Skype and Bittorrent data packets. Bittorrent was chosen because of its high complexity i.e. to increase the overall difficulty.

Taher et al [28] elucidated that demeanor of traffic communication can divulge several parameters such as size and direction of data packet, interarrival time etc, that might disclose user’s identity, activities and private relations or connections. Even with precise adoption of encryption algorithms, it is very difficult to conceal these kinds of information. Such situations are analyzed by traffic analyzers giving them an opportunity to infer characteristics of different users visiting a specific website or application that are running in the wireless networks. In order to preserve the privacy of the user, a defense mechanism and anonymous networks can be used to conceal the traffic patterns and features during communication.

They categorized the traffic analysis into two domains, website domain and wireless domain and also analyzed the traffic analysis technique and its countermeasures. A combination of different suite of layers which illustrates various phases of analysis technique is highlighted with help of integrated process model for analysis of traffic. After this, the factors that may affect the accuracy of the fingerprinting mechanisms are studied for demonstrating how the alteration of these factors can influence the fingerprinting success results. At last, they illustrated various possible challenges that need to be considered when we are planning to implement and deploy it into real-world traffic analysis systems.

Sasikala et al [6] showed that large number of applications that we install on our smart phones
generates huge amount of network traffic patterns. The traffic that is generated by the user while using these applications also contains some characteristic traffic generated by various applications including their background activities or periodic updates or some specific information of particular applications. Although the encryption system presents in various networks for transmitting the data prevents malicious intruders or eavesdropper from getting access to analyze the content of the data, the periodic traffic patterns generated by the applications leak side channel information for instance data packet size, data transfer time and the volume of the data. Since the wireless communications are broadcast in nature various information that can be transmitted like data packet size, its volume, frame size and the modulation scheme used get exposed. This information can be used and exploited by an intruder to passively attack or steal confidential user information. Such kind of problem cannot be avoided even though we encrypt the frame headers and the payloads of the data.

To get access to various transmission attributes of the transmitted data the eavesdropper can cut off unencrypted fields in Physical and MAC headers of data packets. By measuring the frame duration, the intruder can determine the packet size of the frame by estimating the data rate of specific frame. These intruders can find data concerning sources’ and destination machine MAC addresses, modulation scheme and transmission rate of payloads, directions of traffic, length or duration of frame etc [6]. It is difficult to provide social media users with posts that are analyzed from their interests efficiently. It makes it difficult to provide good quality and variety of posts to the users based on their interest. The ever-increasing use and reach of smart phones with an internet connection have enabled to analyze users’ interests from Twitter. Twitter has a huge user base and is used by a large number of people to share posts on a variety of topics and interests as tweets. Mining user’s interests from twitter can increase a number of efficacies like advertisements, trending topics that can be analyzed according to user’s interests and recommendation of posts.

For the same, Jain et al [30] provides an android application which incorporates Web Services, Jsoup, JSON, Firebase Real-time Database and MVC. The application helps to select the posts which include huge images and text that are shown to users as a training set. These personalized posts can later be analyzed by the users themselves using suffix, array ds and artificial neural network. Under ANN, here back propagation methodology has also been used that fires neurons as posts. Kosaraju algorithm and palette lib is also used to help remove redundant posts while also retaining relevant posts with specific hash tags more efficiently and accurately.

3. METHODOLOGY

3.1. Random Classifier Application

The first and foremost task was to select 34 apps which could easily be found and will be used for monitoring passively and cover a wide range of demographics. We are not interested in personal data sets which can be used for identification purposes. Even though, we are not able to infer the personal information of an individual, but we can deduce the data such as age groups, country etc. Information categorized as sensitive is data where additional security is required. The inference generated are only generalized. For instance, most of the people using car trading applications are male while there are few females using those applications as well.

After selecting the applications for studying, there is an issue with measuring app activity like a perspective of external observer. In order to generate more accurate and synchronized results, an external capture mechanism was developed to capture various app activities. A ‘WiFinspect’ [7] app was used for this purpose along with some other readily available software in order to collect data in large quantity with the help of above software used. It is important to note that the test was done with
network used WPA2 (with PSK). Developing a classifier from the data sets is available. A rather subtle technique called “Random Forest Construction” with bigRF package in R [8] [9]. After the development of the app, the process can analyze the usage the accuracy of which can be predicted by the process as a measure of Out-Of-bag (OOB) error. The three-step process of Decision tree construction [10].

This process to deduce the generic information does not make any attempt to break Wi-Fi security measures which is considered as most secured. Thus, these measures only allow us to gather data which is present in the header of the frame and access point (AP). Along with side-channels we can calculate:

- Size of the frame (read starting from header)
- Inter-arrival frame time
- Directions of the frame

With the above information the measurement can be represented as value distributions, Histograms in this case helped to obtain the desired results.

3.2. Inferring User Behavior Without Breaking the Encryption

Most of the communication are done through wireless medium. Kismet (a wireless packet ‘sniffer’) is utilized to execute the observation tasks with a benchmark 802.11b/g wireless network card; in ‘monitor mode’; with Linux drivers. It stores the experiential transmissions as PCAP (Packet Capture) files for scrutiny. We specifically measure the size of the frame and its direction (between the MAC addresses of the receiver and sender). Furthermore, number of frames and frame time slot can be logged. To measure information a program was composed using Sikuli, for imitating actions of various applications under study. This behavior is then logged using the data traffic observer which was described previously. At first, private network behaviors were observed. A 3G mobile device was coupled to a computer, using 802.11g in order to collect Skype [11] traffic. Various other tools such as Hyenae and target devices were used and retained for analysis.

With the measurement and collection of the information we needed to characterize the presence of Skype voice traffic. Only some of the data have the relevant frames and Wireshark Suite can be used to access important packets. Once all the data is filtered. Rest of the process is as follows:

- To generate sliding time windows that is to group different frames received within a given time duration. These windows are used to generate sliding windows at an interval less than the capture time duration of the grouped frames. Thus, a single frame will be present inside some of the overlapping windows which prevents the data loss that can occur if separate windows were used
- A distribution characterizing each metric over the given time duration was used for generating metric distributions for all of the windows.

Statistical picture measures were done to form Distribution over 5s (50 ms distribution of time) Window period. Each of the distribution includes data packets from Skype traffic and is assigned a metric’s score in favor of specified time window (Sw) calculated as follows. The metric score is calculated by taking pre-calculated expected distribution (ei) multiplying with the numbers logged over that time duration with the count monitored on the specified time window (oiw) [12].

\[ S_w = \sum_{i=1}^{n} e_i o_{iw} \]

The numeric scores that would be generated is used to measure Skype-like activity showing the metric
scores over time. A dull background indicates the duration for which a Skype call was underway. Inter-arrival counts were leveled by a factor of hundred for illustration purposes. The most robust pointer of Skype activity is FSize. Metric Thresholds can also be determined during a Skype voice call by metric plot comparisons.

3.3. Frame Encryption by Using Friendly CryptoJam Scheme

Friendly Crypto Jam (FCJ) can be defined as when the jamming signals are amalgamated along with information, after processing digital modulation phase but prior of pushing it to communication channel. The encryption for modulation used for the process preserves the reflected binary (RB) also known just as the Gray Code of the cipher text over the fundamental mapping. This FCJ-encoding is modulation-aware and draws a distinction to standard (digital domain) encoding [14].

Frame detection, FO and CSI detection can be done with the help of physical header since each physical header comes before the preamble. Many replications of visible patterns can be obtained with the help of preamble. Detecting the receival of minimum of two portions of the preamble is required for the estimation of FO. By considering replications in received signal like a benchmark testimonial and weighing it against alternative replications, with T seconds delay, a frame can be decoded. CSI estimation can be performed by comparing the known patterns in preamble with its received value.

An adversary can intercept the preamble, physical and MAC headers since all of the headers are sent during the transfer of information. Based upon the channel specifications; communication rate for the frame payload (including MAC header) is attuned, whereas the preamble and the physical layer header are communicated at the least supported rate. It results in variation of frame time (in seconds) for similar payload. The ‘Coding and Modulation Scheme’ in 802.11n, signify both the pace rate of encoding and methods of modulations, akin to ‘rate’ of 802.11a. All 802.11 alternatives identify a ‘length’ attribute, that symbolizes payload size in octets (for 11a/n) or in milliseconds (for 11b) [15].

Any kind of rate-based SCI classification can be prevented if the scheme which is for the modulation purpose of different frame payloads always investigate it. This can be achieved as a result of implanting payload’s primary modulation codes in assembly chart of maximum directives of modulation scheme.

3.4. Website Fingerprinting Technique

A number of experiments have been conducted in different papers to show that an improvement is still needed in existing traffic analysis countermeasures. Wagner and Schneier [16] introduced an earliest endeavor in assailing website traffic for recognizing identities of users. The random padding method used in SSL protocol works in block-cipher modes only, that permits cipher text to disclose plain text segments. For inferring the identities of the visited website this shortcoming has been used effectively. [16] Owing to this loophole, it was suggested to adhere to random length padding for all cipher modes towards resolving the problems in SSL.

Sun et al [17] also concluded that a considerable amount of information can be revealed from the encrypted communication. Bissias et al [18] conveyed another noteworthy construct, for a year they collected data packets with the use of OpenSSH tunnel coupled Firefox. After selecting the inter-arrival time & the packet size, similarity of the two traces of different time gap packets was recognized and a cross-correlation metric was generated. The obtained results were quite good despite of low success rates. Levine et al [19] developed two novel methods to fingerprint websites traffic; exploiting Naive Bayes (NB) classifier beside density estimation. The experiments conducted, showed that there is a need to secure OpenSSH protocol in order to block the threats from attackers so that they cannot
analyze the traffic passing through it.

Shi et al. [20] introduced a method for fingerprinting of websites which can be used to probe traffic transmissions on Tor. They divided the different direction of packets of data in numerous intermissions and converted them into vectors. Using, Cosine Similarity formula, resemblances are calculated between experimental vectors and distinguished fingerprints. The generated results employing above technique was then evaluated in theory as well as practically in order to demonstrate how effective the method is for generating vulnerability to user's anonymity as compared to Tor.

Zhang et al. [21] designed an innovative fingerprinting method to attack websites where data was accumulated by seizing packets awaited from browsing websites by Firefox linked through Tor exploiting Tshark. Every website was browsed a number of times with the intention of collecting a great amount of trace packets. To identify visited websites Damerau-Levenshstein Distance algorithm was deployed. They were found the volume, arrangement, directions and supplementary helpful data of packets with the classifier help. Additionally, Hidden Markov Model was also used to identify. These experiments demonstrated there is a need to improve the existing security models aligned with Tor traffic analysis. Seeing the outcome, Congestion-Sensitive BuFLO which was considered an improved defense scheme was introduced by them. As shown in their work, it provides better security systems than its predecessor.

Wang and Goldberg introduced Optimal String Alignment Distance (OSAD) attack based on the attack proposed by Zhang [21] that is essentially an enhanced adaptation of their so-called Cai’s fingerprinting attack. This new metric was proposed to identify the likeness amid two packets of traffic data stockpiled using Firefox exploiting Tor. By eliminating the SENDME packets from Tor cells, higher accuracy can be achieved. These experiments were carried over real world accessible websites, akin to Panchenko [22], and might produce better outcomes. By combining the attacks designed by Zhang [21] and Wang; another fingerprinting attack was pioneered. The resulting technique got a higher success rate than preceding techniques in precision and procedure duration. These tests were performed in real world scenarios over large open world information assembled using Tor.

3.5. Wireless Fingerprinting Technique

Ever since the introduction of wireless communication, WLANs are an ever-present part of our society. With the increase in the use of WLAN, it has become easy for adversaries to snoop and analyze the user traffic over WiFi links even though the encryption is deployed perfectly in the communication system. By analyzing and observing the specific patterns in various packets about the characteristics and behavior of the transmitted packet the intruders were able to surmise online and local activities of users. It is difficult to extract traffic features while user is operating additional applications simultaneously due to interference of applications packet between each other.

The encoded VoIP calls were identified by a new method which was introduced by Wright et al. [23] The phrases spoken during call conversations can be identified through the packet dimensions of encoded VoIP signals. This method adopted a mechanism called Hidden Markov Models representing the purpose of distinguishing 122 objective sentences that are edified using training data of TIMIT. An accuracy more than 90% was achieved using this method.

A fusion procedure was proposed for network traffic classification by Tavallaee et al [24]. Few machine learning techniques and signature-based method was applied in this mechanism. A hierarchical classification based system was introduced by Zhang et al. [25] to infer online activities of
various users. In order to analyze the identity of users that uses encrypted wireless communication, Atkinson et al. [26] projected a procedure. The experiments were carried out by running users’ apps and then gathering information through actions replication of several users. These packets are first gathered and then identified by a specific set of metrics such as the size of the packet and inter-arrival time. At last, the traffic is extracted by applying aggregate normalized distributions over each metric. Multiple accuracies were gained based on the number of packets collected.

3.6. Neural Networks Back Propagation

Neural Networks Back Propagation implemented in amalgamation with an optimization method is a widespread technique of training Artificial Neural Networks. It is used for calculating the loss function gradient w.r.t to the weights present in the network. Attempting to curtail the loss function, a gradient is used with the optimization method that further updates the weights. Backward Propagation requires a desired input known with the method for every input to compute the loss function gradient; therefore, generally contemplated as supervised learning method. It can moreover be employed in several unsupervised methods like auto-encoders. Back propagation is used for proper arrangement of user's posts.

![Neural Network](image)

**Figure 4** Neural Network

3.7. Kosaraju Algorithm

It is a depth first search algorithm. If a path exists among each and every one vertices pairs; the graph is entitled a strongly connected directed graph. Maximal strongly connected sub-graph is a Strongly Connected Component of a directed graph. [27]

![SCC Graph](image)

**Figure 5. SCC Graph**
DFS is done twice here. A single tree is produced by a DFS of a graph if all vertices are reachable from the DFS starting point. In the next step, the graph is reversed. Here the algorithm is used for removal of redundant posts. The vertices are marked as not visited and are filled in a stack according to their finish time in the first DFS. In second DFS, the vertices are marked as non-visited. All the vertices are processed in an order as defined in the stack. Vertices are then popped from the stack and the SCC [28] of the popped vertex is printed out. In the next step, the direction of the pointing to SCCs are reversed.

4. CONCLUSION

This paper highlights that even though various Wifi encryption techniques works perfect as intended, sensitive and personal information of the users are still at the risk of getting broadcasted whether intentionally or unintentionally. A distant and untraceable detection mechanism is deployed by the intruders in order to gather user’s private information by observing the network activity of the encrypted app. It is possible to infer and detect user behavior to an extent by an external and entirely passive user, despite providing only limited data and using correct encryption techniques. It is difficult to design efficient protocols that resist the analysis. Side effects of efficient networking such as variable frame size and inter-arrival times cannot be ignored.

The methods and the corrective measures used for analyzing traffic and fingerprinting have also been reviewed here. They have been divided in two realms; wireless and websites. We have shown that existing security mechanisms, encryption protocols, & anonymity networks do their paramount for concealing personal and private data of users. We have also demonstrated how malicious users utilize all possibilities to analyze and study application traffic of users in order to disclose their identities.

The prevention of transmitting attributes like visible PHY/MAC header fields and the modulation scheme of payloads is a difficult task. Friendly-CryptoJam (FCJ) efficiently safeguard confidentiality of lower-layer attributes & avert SCI- based traffic classification, rate-adaptation, dictionary, plaintext, modulation detection, and device-based tracking attacks [6]. With wireless communication becoming increasingly common, and commercial companies becoming keener in tracing and analyzing publicly transmitted wireless data, this paper therefore presents an important and demonstrable threat to user's privacy.

References

[1] Your WiFi is leaking By: John S. Atkinson, John E. Mitchell, Miguel Rio, George Matich
[2] H. Zimmermann, OSI reference model—the ISO model of architecture for open systems interconnection, IEEE Trans. Commun. 28 (4) (1980) 425–432.
[3] IEEE-SA, Wireless LAN Medium Access Control, MAC, and Physical Layer, PHY, Specification, IEEE Standards Authority, 2007.
[4] N. Lawson, Side-channel attacks on cryptographic software, IEEE Secur. Privacy Mag. 7 (6) (2009) 65–68.
[5] A. Lim, L. Breiman, A. Cutler, bigrf: Big Random Forests: Classification and Regression Forests for Large Data Sets, 2013.
[6] Mrs. G. Sasikala, Mrs. D.Kavitha Full Frame Encryption and Modulation Using Friendly CryptoJam Scheme
[7] A. Hadjittofis, WiFinespect Play Store Page, 2014. https://play.google.com/store/apps/details?id=uk.co.opticiancms.wifiprobe.
[8] L. Breiman, Random Forests, Mach. Learn. 45 (1) (2001) 5–32.
[9] L. Breiman, Random Forests, 2013, http://www.stat.berkeley.edu/~breiman/RandomForests/cc_
[10] R Core Team, R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria, 2013.

[11] S. A. Baset and H. G. Schulzrinne, “An analysis of the skype peer-to-peer internet telephony protocol,” in INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings. Apr. 2006, pp. 1–11.

[12] F. Zhang, W. He, X. Liu, and P. G. Bridges, “Inferring users’ online activities through traffic analysis,” in Proceedings of the fourth ACM conference on Wireless network security, ser. WiSec ’11. New York, NY, USA: ACM, 2011, pp. 59–70.

[13] A. White, A. Matthews, K. Snow, and F. Monrose, “Phonotactic reconstruction of encrypted VoIP conversations: Hookt on fon-iks,” in Security and Privacy (SP), 2011 IEEE Symposium on, may 2011, pp. 3–18.

[14] C. Cardoso, A. R. Castro, and A. Klautau, “An efficient FPGA IP core for automatic modulation classification,” IEEE Embedded Syst. Lett., vol. 5, no. 3, pp. 42–45, Sep. 2013.

[15] IEEE-SA. Wireless LAN Medium Access Control, MAC, and Physical Layer, PHY, Specification, IEEE Standards Authority, 2007.

[16] Wagner, D., Schneier, B.: Analysis of the ssl 3.0 protocol. In: The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 29–40 (1996)

[17] Sun, Q., Simon, D.R., Wang, Y.M., Russell, W., Padmanabhan, V.N., Qiu, L.: Statistical identification of encrypted web browsing traffic. In: Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on, pp. 19–30. IEEE (2002)

[18] Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N.: Privacy vulnerabilities in encrypted http streams. In: Privacy Enhancing Technologies, pp. 1–11. Springer (2006)

[19] Liberatore, M., Levine, B.N.: Inferring the source of encrypted http connections. In: Proceedings of the 13th ACM conference on Computer and communications security, pp. 255–263. ACM (2006)

[20] Shi, Y., Matsuura, K.: Fingerprinting attack on the tor anonymity system. In: Information and Communications Security, pp. 425–438. Springer (2009)

[21] Cai, X., Zhang, X.C., Joshi, B., Johnson, R.: Touching from a distance: Website fingerprinting attacks and defenses. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 605–616. ACM (2012)

[22] Panchenko, A., Niessen, L., Zinnen, A., Engel, T.: Website fingerprinting in onion routing based anonymization networks. In: Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp. 103–114. ACM (2011)

[23] Wright, C.V., Ballard, L., Coull, S.E., Monrose, F., Masson, G.M.: Spot me if you can: Uncovering spoken phrases in encrypted voip conversations. In: Security and Privacy, 2008. SP 2008. IEEE Symposium on, pp. 35–49. IEEE (2008)

[24] Tavallae, M., Lu, W., Ghorbani, A.A.: Online classification of network flows. In: Communication Networks and Services Research Conference, CNSR’09. Seventh Annual, pp. 78–85. IEEE (2009)

[25] Zhang, F., He, W., Liu, X., Bridges, P.G.: Inferring users’online activities through traffic analysis. In: Proceedings of the fourth ACM conference on Wireless network security, pp. 59–70. ACM (2011)

[26] Atkinson, J., Adetoye, O., Rio, M., Mitchell, J., Matich,G.: Your wifi is leaking: Inferring user behaviour, encryption irrelevant. In: Wireless Communications and Networking Conference, pp. 1097–1102. IEEE (2013)

[27] Kim, J., Hastak, M. (2018). Social network analysis. International Journal of Information Management: The Journal for Information Professionals, 38(1), 86-96.

[28] Alshomrani, S., & Iqbal, G. (2012). Analysis of Strongly Connected Components (SCC) Using Dynamic Graph Representation. International Journal of Computer Science Issues, 9(4).
[29] Taher Ahmed Ghaleb (2016) Techniques and countermeasures of website/wireless traffic analysis and fingerprinting. Journal of Cluster Computing. Vol. 19, Issue 1, 427-438

[30] A. Jain, A. Gupta, N. Sharma, S. Joshi, and D. Yadav, “Mining application on analyzing users’ interests from Twitter,” In Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), IEEE, March, 2018.