International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-8, Issue-12)

Research Article | **December 2018**

A Case Study of IP Camera Monitoring Traffic Verification

Reem Alshalawi[1], Mohamed Osama Khozium[2]
[1]*Master of Computer Science, Umm Al- Qura University, Makkah, Saudi Arabia*
reem1@usa.com
[2]*Professor, Department of Engineering & Applied Science - Computers, MCC, Umm Al-Qura University, Makkah, Saudi Arabia*
osama@khozium.com

Abstract: ***Technology takes apart of our daily life, it also became a confidant of our privacysuch as thesurveillance camera which is available everywhere andits presence has prevented many cases of robberies and crimes. Despite the wide spread of IP camera, a serious drawback is present in it, where there is the probability of being hacked and therefore there will always be the fear of being under threat.***

In this paper, the IP camera traffic will be monitored to detect if there is any attack that stopped the camera from work, we proposean algorithm that splits the IP camera traffic into a set of streams, then calculates the time difference and its mean for each stream to determine whether the camera is attacked or not.

After calculating the standard deviation which affects positively on reducing the false alarm, the results showed high accuracy which reflects higher level in security and more confidence inIP camera performance.

Keywords: Camera Forensic, surveillance camera security,illegal access, monitoring data traffic, wireless camera

I. INTRODUCTION

The rapid development of technology led to giving every device its own IP address to connect to the internet no matter what the type is. The trend in surveillance cameras is using the IP camera, however there isalways the fear of being under threat. Most of the users that need surveillance camerasprefer Closed Circuit Television (CCTV) cameras to IP cameras, despite the many advanced features of IP cameras because of the security and privacy issues [1],[2],[4]. Actually, IP camera has security issues as other devices which connect to the Internet [1],[2],[3].

The attacks on household IP camera are classified as non-critical facilities and the level of attacks accord many studies and analysis results are differ among high level and medium level.

Many studies have stressed the need to ensure surveillance IP camera and other house devices of security attacks, which are subjected to intensive existence of strong threat to the privacy and security of users. These studies determined that IP cameras, like other devices that are connected to Wi-Fi, are vulnerable to hacking, blocking, and spying, which disrupts their work or reflects their function [3].

Therefore, the aim is to monitor camera traffic and detect if there is any attack that stopped the IP camera from work. We designed an algorithm that will help investigators to find any missing in the camera data traffic.

This paper is organized into five sections; first section was the introduction, second section is about related works presenting many researches that are concerned about privacy and security issues for surveillance camera and monitoring data traffic, third section is an overview of IP camera and its characteristic, fourth section shows our case study, and finally, the fifth section where there is the present conclusions and future work.

II. RELATED WORK

There are recent works which have focused on monitoring network traffic and surveillance camera investigation, some of these works study the possible attack and some others study traffic behavior network traffic [2], [3], [5],[15].

In [5] Sivanathan et al. monitored a set of traffic devices connected to a specific network for a period of continuous months in real time and used machine learning to categorize and diagnose the types of these devices. This proposed system showed very high results in accuracy as well as being the first leading system to categorize and diagnose devices with this mechanism. See Figure 1.

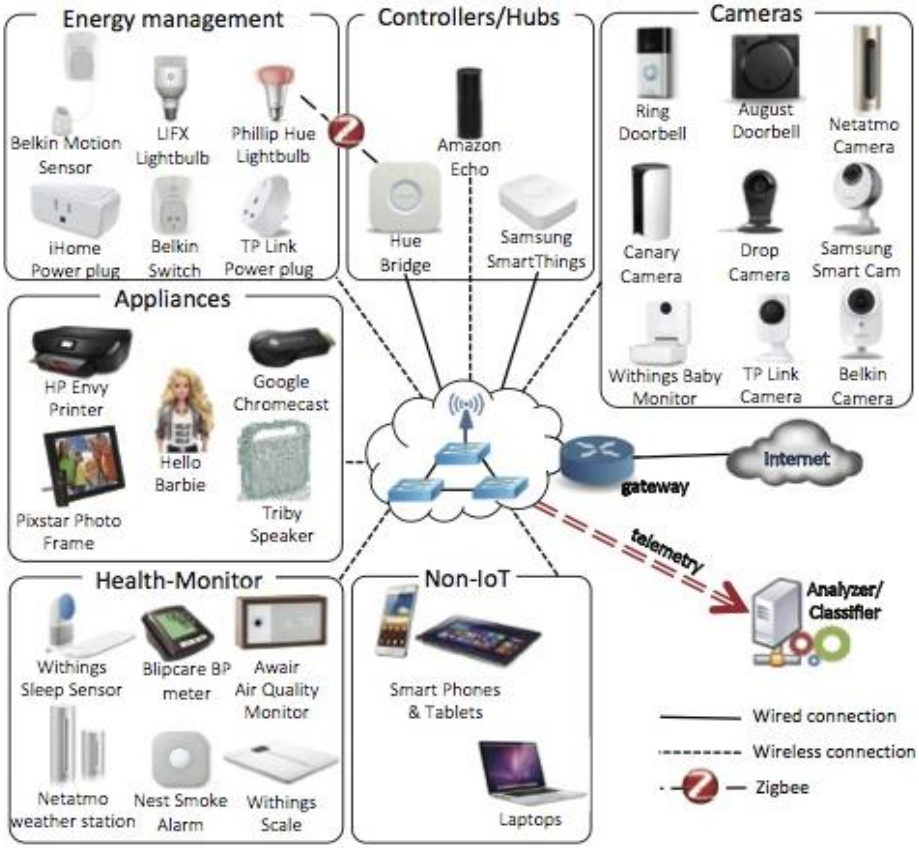

Figure 1: The model of categorized in [5]

Alshalawi et al. in [2] suggested a tool to investigate unauthorized access to wireless camera. They designed two algorithms to identify the duration time of camera traffic and legal IP addresses that is authorized to communicate with wireless camera. See Figure 2.

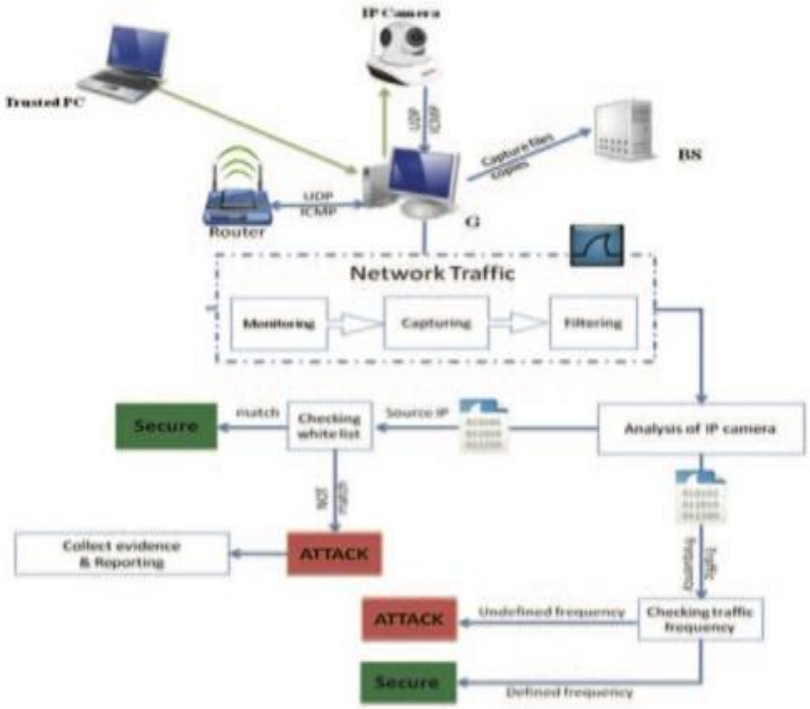

Figure 2: Investigation tool of work [2]

Another proposal [6] designed an UPnp-based Surveillance Camera System (USCS) which provided the authority of managing local network and its traffic by using UPnp technology beside allowing remote access for their system by using Open Service Gateway initiative (OSGi). USCS ensured safety and security for household usage.

The work in [7] built a system that mainly focuses on monitoring the internet protocol traffic between local area network and Internet. Their system presented to detect unauthorized IP addresses that are in the network range. The proposed system had ten modules to make user interaction with the system easier. As a result, this system was successfully built to detect and block the unauthorized access in the network.

Shanklin et al. in [8] designed a system which monitors the incoming and outgoing data traffic for many ports in the network. The system denied unauthorized data that goes through the ports.

A rules table determined the allowed data packets that can passed from or to the ports. The system keeps dynamically updating the rules table to specify future illegal access for data packets.

Ji et al. in [9] studied the new idea of attackers that can discover if the users are inside the house or not. Their work proposed a HomeSpy system that generates user presence by examining the fundamental pattern of wireless camera movement. To find out if there is a user, HomeSpy dives wireless data traffic around the target home and monitors if there are wireless cameras with LSTM,then HomeSpy applies an algorithm which depends on cumulative sum control chart to find out if there is a user inside the house.

Security model in [10] is to use three different levels of access to detect any suspicious behavior which is classified into two types: classified attack and unclassified attack. Their model aimed to secure data warehouse from illegal access.

AbdAllah et al. [11] designed an access control of elliptic curve for ICN architectures. They did some analysis in various attacks such as: man in the middle attack and privacy breach. As a conclusion of their research, the proposed design prevented illegal access to ICN contents.

In this method [12] Tran et al. suggested a method that controls the access on a hotspot of smart phone. This method detects illegal access of any device communicated to that hotspot of the smart phone by the analysis of illegal access of data signatures. The method includes controlling the illegal data movements and redirecting the user of smart phone to a restricted gateway to support the allowed connection plan.

Masoud et al. in [13] studied the consequences of anomalous violations in wireless networksand proposed an algorithm that detects user behavior which is Hybrid Network Intrusion Detection. Their approach is based on two algorithms: genetic algorithms and estimation maximization.

III. OVERVIEW OF IP CAMERA

Surveillance camera has several types and purposes. The most common systems are IP camera and CCTV camera and until now both are used. Actually, a lot of people still don't trust IP camera system despite the fact that it has better characteristics, which exceeds CCTV cameras.

A Comparison of characteristics between analog and IP cameras during video surveillance system performance is shown in table 1. [1]

Most of people believe that CCTV cameras are more secure, in contrast than the IP camera which sometime maybe under threat and used by attacker as a spy!

With the technological revolution in the world, the trend of IP cameras has become the dominant because of its sophisticated characteristics, which digitize the video signals inside the camera itself, unlike the older types of cameras [2], [4].

Table 1: Comparison of characteristics between analog and IP cameras

	Scenario with analog cameras	Scenario with IP cameras
Camera resolution	from 420 to 700 TV lines, 4CIF resolution	from 1 MPixel to 8 MPixel
Cabling (Video and Power)	coaxial to each camera and DVR, additional power cables	Cat 5e, Power over Ethernet (PoE)
The average cable length	100 m/camera (video) 65 m/camera (power)	65 m/camera (Cat5 with PoE)
Power	Power for cameras	PoE
Switches	to all types DVR	PoE switch
Server / memory	Mid-end DVR (H.264 compatible with memory)	PC (standard) with memory
Software	on the DVR (H.264 compatible)	AXIS Camera Station
Monitors	standard high resolution monitors	standard high resolution monitors

Table 2 shows the specification of the used IP camera. [11]

Table 2: Specification of the IP camera

Model		UIP-IHF1028-B10
Device	Device Type	1.0 Megapixel CMOS Sensor 1/4"
	Day&Night	Yes
	Color	0.5lux (IR ON)
	IR Cut Filter	Support
	IR Distance	8-10Mvvvc
Lens	Lens	3.6MM
	IRIS	Fixed Aperture F1.2
	Viewing Angle	Pan: 355°/ Tilt: 90°
Video	Compression	H.264
	Resolution & Frame	Main Flow: 1280*720@30fps Minor Flow: 640*360@30fps
	Code Stream	Support Dual Stream
	Code Rate	32-4096kbps
	Bit Rate Type	CBR & VBR
	SNR	Above 50DB
Alarm	Audio	1 CH Two-way-audio Built-in Mic External Output Device
	Alarm In/ Out	1CH
	Ethernet Port	Ethernet (10/100 Base-T),RJ-45 connector
Software	Intelligent Software Function	Motion Detect, Miss Object Detection,Suspicious Detection, Moving Object Tracking, Guard Line Detection, etc.
	Event Action	Video Capture Saved to Backing Device, Send Email, Send SMS, Zoom in alarm, Pop ap map, Go to PTZ preset pos etc
	Remote Access	DDNS, software, P2P
General	Power Consumption	DC 5V/2A
	Operation Temperature	-10°C——60°C
	Operation Humidity	10%-80%
	Dimensions	103(L)*75(W)*125(H)mm

IV. CASE STUDY

IP camera runs all the time and it is supposed to send traffic so that any missing of this traffic means that there is an attack. We pave the process of detecting any attack that aims to disable IP camera, we help the investigators by studying IP camera traffic behavior and provide an algorithm that facilitates this type of attack detection. See Figure 3

4.1 Algorithm

Our algorithm studies the deliver time of camera traffic, and it is called Deliver Time Calculating (DTC). DTC deals with camera log-file and reads the set of camera traffic. We split camera traffic to set of streams, each stream has different transmit time,shown in Figure 3. DTC calculates the time difference between the streams of traffic. After that DTC computes the mean and the standard deviation. Then DTC generates the base time and afterwards it does the comparison. If the result of difference time is greater than the base time we obtain an attack otherwise it is secured. See Figure 4 the DTC algorithm.

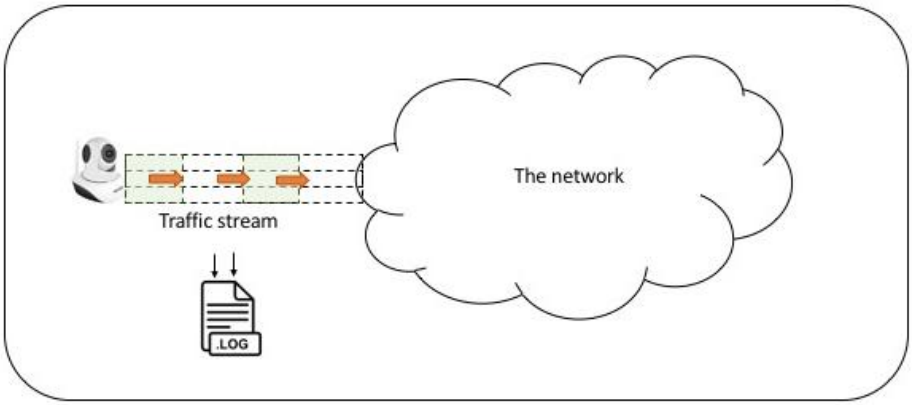

Figure 3: Three IP camera stream of traffic

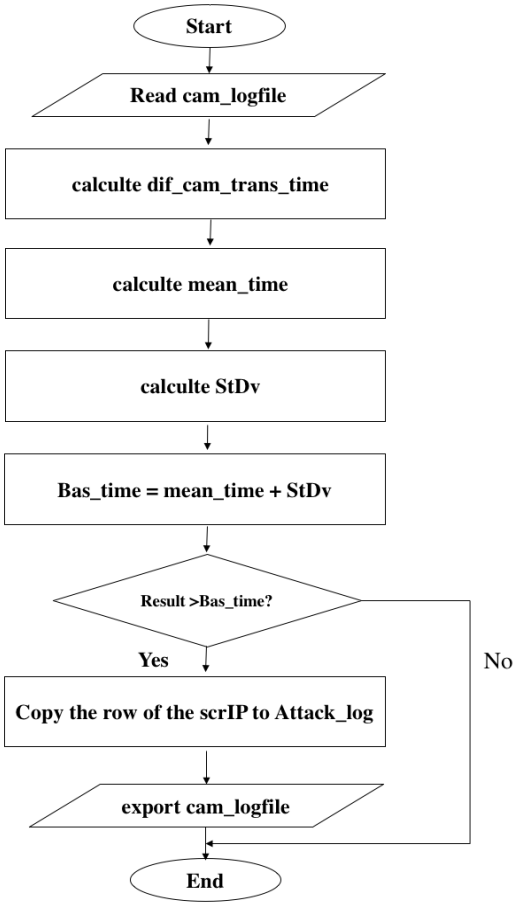

Figure 4: DTC algorithm flow chart

4.2 Calculating The Base Time

We have captured a set of camera traffic = 1000 transaction process and as we mentionedbefore, camera generates traffic all the time.

Figure 5 shows a set of stream difference from our case study.

The mean = $\frac{\Sigma stream\ \ difference}{number\ \ of\ streams} \approx 19$

The standard deviation = $\sqrt{\frac{\Sigma(stream\ \ difference\ )^2}{number\ \ of\ stream}} \approx 17$

Our casebase time = the mean + the standard deviation = 36

374.701195000	374.705856		18.447265000
374.710791000	374.715494		
374.720278000	374.724668		
374.729162000	374.733449		
374.737760000	394.913316		
394.913404000	394.913526		20.202735000
394.913822000	394.913861		
400.084182000	400.084215		
434.900774000	434.900921		
434.901048000	434.901232		
434.902711000	434.902747		39.988925000
434.903333000	434.903364		
474.428385000	474.428472		
474.428588000	474.429239		
474.429289000	479.549358		
479.549375000	494.91156		60.008227000
494.916409000	494.921251		
494.925943000	494.930781		
494.935484000	494.940271		
494.944611000	494.948935		
494.953219000	494.957529		0.041120000
514.365367000	514.365513		
514.365641000	514.366211		
514.367953000	514.367991		
514.369086000	514.369116		
553.174721000	553.174817		38.809450000
553.174933000	553.175366		

Figure 5: Set of stream from case study log file

4.3 Result

We measure DTC performance by precision and accuracy and we use confusion matrix elements true positive (TP) rate, false positive (FP) rate, true negative (TN) and false negative (FN).

TP indicates that the comparison result is labeled correctly

FP indicates that the comparison result is labeled incorrectly

TN indicates that the comparison result does not show the attack case when the base time is smaller than comparison result.

FN indicates that the result of comparison shows no alarm.

Table 3 has TP, TN, FP and FN rates values.

The mean of difference time could be used as a measure to check the deliver time of traffic,represented in figure 6.

The standard deviation had been calculated and it was noticed that high accuracy was achieved and false alarm is reduced, as illustrated in figure 7 & 8.

Table 3: The values of TP, FP, TN and FN rates

Difference Time	Result Comparison with Base Time		TP	FP	TN	FN
7.080137000	< 36	Secure	1	0	0	0
0.001237000	< 36	Secure	1	0	0	0
40.544725000	> 36	Attack	0	1	0	0
19.453932000	< 36	Secure	1	0	0	0
5.119764000	< 36	Secure	1	0	0	0
43.627851000	> 36	Attack	0	1	0	0
13.004484000	< 36	Secure	1	0	0	0
2.278766000	< 36	Secure	1	0	0	0
39.525021000	> 36	Attack	0	1	0	0
38.805605000	> 36	Attack	0	1	0	0
60.008227000	> 36	Attack	0	1	0	0

Precision = $\frac{TP}{TP+FP} = \frac{995}{995+5} = 0.995$

Accuracy = $\frac{TP+TN}{TP+FP+TN+FN} = \frac{995+0}{995+5+0+0} = 0.995$

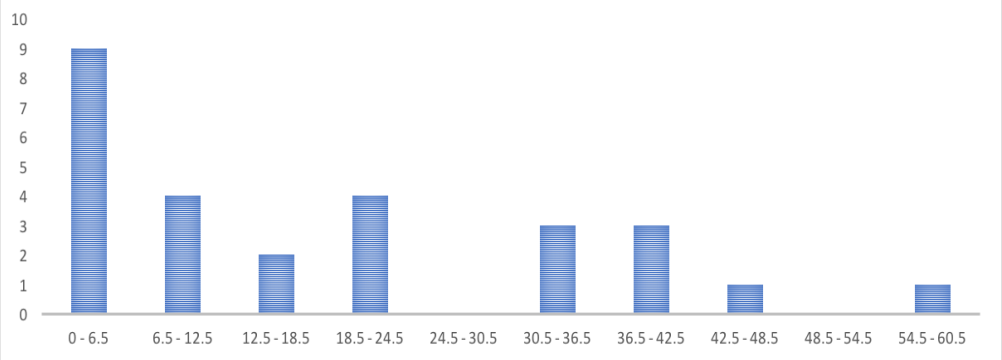

Figure 6: The mean representation

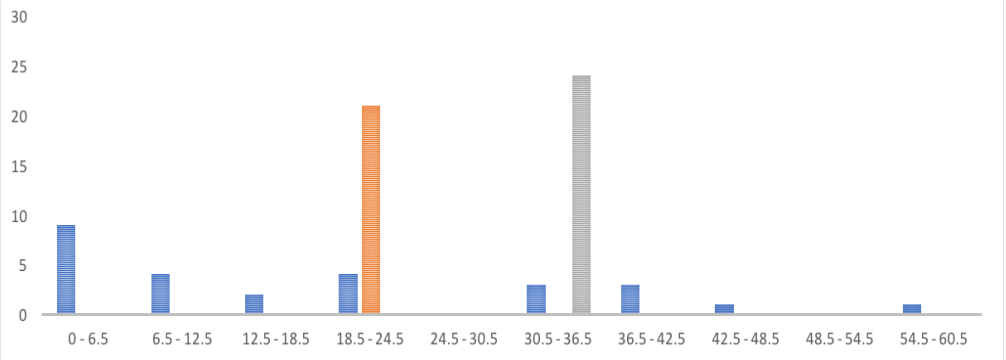

Figure 7: The standard deviation representation

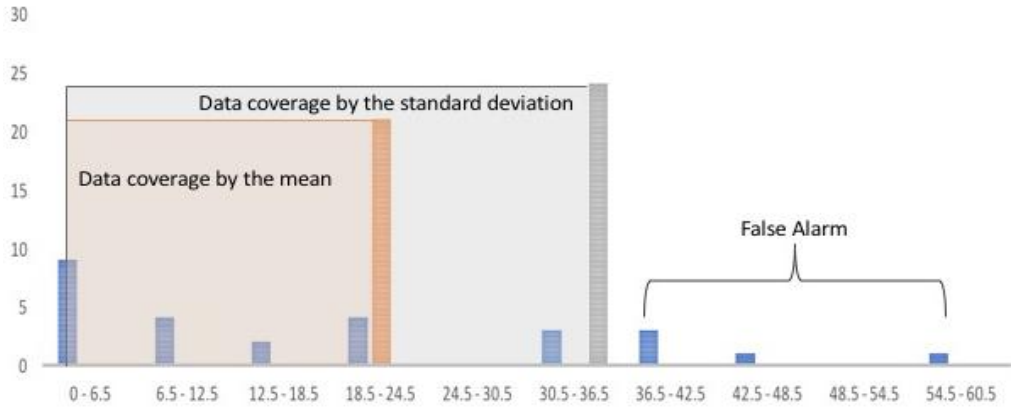

Figure 8: Coverage data including mean, the standard deviation and false alarm representation

We obtain a high score in precision and accuracy which reflects the high performance for DTC.

V. CONCLUSIONS AND FUTURE WORK

Improvements have been done into the algorithm of CTTC to minimize the false alarm and raise the security level as possible. Current algorithm supports the privacy and security more than the previous for IP camera which is easily run and easier in work. In the future, we can add immune system that can create a profile for each IP camera on the system to becompatible with more than one set of IP camera work in local network or remote network.

REFERENCES

[1] V. Memos, K. Psannis, Y. Ishibashi, B. Kim and B. Gupta, "*An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework*", *Future Generation Computer Systems*, vol. 83, pp. 619-628, 2018.

[2] R. Alshalawi and T. Alghamdi, "*Forensic tool for wireless surveillance camera*", 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017.

[3] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "*A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services*", IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3453-3495, 2018.

[4] GradimirkaPopovic , NebojsaArsic , BranimirJaksic , Boris Gara , Mile Petrovic, "*Overview, Characteristics and Advantages of IP Camera Video Surveillance Systems Compared to Systems with other Kinds of Camera*", International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 2, no. 5, 2013.

[5] A. Sivanathan, H. HabibiGharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath and V. Sivaraman, "*Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics*", IEEE Transactions on Mobile Computing, pp. 1-1, 2018.

[6] Y. Gu, M. Kim, H. Lee and O. Choi, "*Design and Implementation of UPnP-Based Surveillance Camera System for Home Security*", *IEEE*, 2013.

[7] I. A Hamid, N. AbSukor, C. MohdFoozy and Z. Abdullah, "*Network Monitoring System To Detect Unauthorized Connection*", Acta Electronica Malaysia, vol. 1, no. 2, pp. 13-16, 2017.

[8] P. Billquist, D. Sodman, G. Garbutt, M. Nadler and C. Shanklin, "*Method and device for monitoring data traffic and preventing unauthorized access to a network*", us20020133586, 2018.

[9] X. Ji, Y. Cheng, W. Xu and X. Zhou, "*User Presence Inference via Encrypted Traffic of Wireless Camera in Smart Homes*", Security and Communication Networks, vol. 2018, pp. 1-10, 2018.

[10] G. Kumar, K. Ahmad, A. Kumar Saurabh and M. Doja, "*Data Prevention from Unauthorized Access by Unclassified Attack in Data Warehouse*", International Conference on Computing for Sustainable Global Development, 2014.

[11] E. AbdAllah, M. Zulkernine and H. Hassanein, "*Preventing unauthorized access in information centric networking*", Security and Privacy, vol. 1, no. 4, p. e33, 2018.

[12] D. Tran, K. Warmerdam, T. Lim, R. MacPherson and B. Singh, "*Managing tethered data traffic over a hotspot network*", 2015.

[13] M. Masoud, Y. Jaradat and I. Jannoud, "*On Detecting Wi-Fi Unauthorized Access Utilizing Software Define Network (SDN) and Machine Learning Algorithms*", International Review on Computers and Software (IRECOS), vol. 12, no. 1, p. 21, 2017.

[14] "UIP-IHF1028-B10 - UXD Technologies Ltd.", *UXD Technologies Ltd.*, 2018. [Online]. Available: http://www.uxdsecurity.com/product-detail/uib-ihf1028-b10/. [Accessed: 09- Dec- 2018].

[15] Mohamed Osama Khozium, "*Hello Flood Counter Measure for Wireless Sensor Net works*", International Journal of Computer Science and Security, volume (2) issue (3), may-june 2008.

