Jamming Attack – A Survey

Kirti Sharma[1], Shobha Bhatt[2]

Ambedkar Institute of Advanced Communication Technologies and Research, Delhi

[1]kkirti.sharma@yahoo.com

[2]bhattsho@gmail.com

***ABSTRACT*- In this digital world, IoT is grabbing the major part. Every initiative related to the Wireless Sensor Network has the backbone as IoT. IoT is specialized in sensing, network connectivity, software and electronics. It allows items to be controlled or sensed remotely across the wireless network. With the advancement of this technology, the sensor network in wireless is bared to several types of attacks such as active and passive attacks. As it includes the wireless communication so it is more prone to eavesdropping and interception of signals. In wireless sensor network, nodes are susceptible to jamming. This paper represents a study on various jamming attacks relied on either physical layer or MAC layer. Then further various countermeasures for mitigating from these attacks are discussed.**

***Keywords*- Jamming, proactive jammers, reactive jammers, intelligent jammers, Websploit, WSN.**

I. INTRODUCTION

Jamming attack is possible there, where frequency is used. In WSN, the whole communication is frequency based as there is no linking among nodes like in physical media communication. IoT is specialized in sensing, network connectivity, software and electronics [1]. One major characteristic of WSN is the broadcasting behavior. This makes them susceptible to attacks which further leads the network performance degraded and various intrusions. One such attack is Jamming, this is considered to be the rigorous Denial-of-service where the channel medium is crashed via sending many requests to the server, or interrupting in the communication to further drop or not allow the responses to reach to the target. Due to which the client ponders that the server is not retorting to the request and then he continuously sends the requests to get the response from the server [2]. Unlike the regular attacks, this attack is accomplished after reconnaissance. The attacker requires the detailed knowledge about the communication pattern. He listens to the traffic and sends the jammed signals continuously to obstruct the conduit [2] and interrupt the transmission medium to resist the intended data to be reached at target. This disruption of communication results to jamming attack. In a survey paper of MAC layer Jamming attack, authors discussed about the intelligent jammers. MAC protocols are exposed to these kinds of jammers. On the basis of the pattern of communication, a jammer can pick the right area for the attack purpose. Initially, it selects the region with the highest communication flow and then it commences an attack [3]. Thus, this causes the neighboring nodes to suffer the most. This leads to high cost of action with a low message delivery rate. As the smart jammer might have access to control over the channel. It starts sending the continuous jammed signals in order to block channel negotiation. Moreover, it can extort the sequence of next control channels from legitimate nodes, which will smash up the whole network. Accordingly, there is coinciding between the jammed signals and the packets sent from valid network nodes. In most wireless networks, collision is caused due to two nodes sending data at the identical instance on the same conduction medium [5].

II. JAMMING ATTACKS

Under this heading, jammers are categorized into two domain fields: Fundamental jammers and intelligent jammers. But, technology wise, these are segregated into proactive and reactive ones.

A. *Fundamental jammers*

Fundamental Jammers mainly comprises four kinds of jammers: constant, random, deceptive and reactive. Constant jammer is physical layer based while the remaining ones are MAC layer based. Constant jammer constantly emits the radio signal as there is no means to work only then when there is either communication or not. It sends the random bits continuously exclusive of any label of MAC. Deceptive jammers constantly inject normal packets to the conduit with no space during transmission of consecutive packet. Therefore, a nodule will be duped into believing that the packets it is receiving, is a genuine packet and would stay in the receipt state. That means a usual conversationalist will be deceived into receiver state. Random jammer switches between sleep mode and jam mode. The times of attack and sleep can vary, which allows a wicked node to attain diverse levels of compromise between energy-efficiency and the efficacy of jamming, while depending on the application. Reactive jammers settle quietly when there is idle channel. They mainly start their working when they sense that network has started its activity.

B. *Intelligent jammers*

The jammers who target the physical layer are basically designed to destroy the signal, congest the network and require the nodes to consume more energy. While the other jammers targeting the MAC layer are supposed to attack the network privacy. Their objective is to determine the MAC protocol used by victim nodes in order to launch an energy-efficient attack. Numerous clarifications have been projected to counter the jammers related to MAC layer level such as frequency hopping, sequence of frequency, packet fragmentation, frame masking and redundant coding to diminish the brunt of damage caused by a jammer.

III. JAMMING TECHNIQUES

Wireless communication is hindered by intended radio interventions originated by jamming to maintain the communication conduit busy. This leads a source to back-off every time whenever it senses the medium busy.

A. *Types of jammers*

Jammers are actually malicious nodes in wireless that cause deliberate interference in the wireless network whenever planted by any anonymous user. These jammers are partitioned among proactive and reactive.

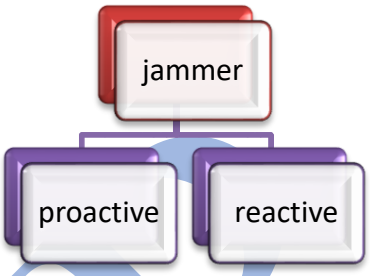

Fig. 1 Types of jammer

1) *Proactive jammer* -It works whether the data communication is there or not, sends jamming (interfering) signals in a network.

a. *Constant jammer*- Instead of following the CSMA protocol, random bits are emanated continuously by constant jammer. According to the CSMA mechanism, before transmitting any data onto the channel, a valid node has to sense the status of the wireless medium [9].

b. *Deceptive jammer*- Instead of releasing random bits (as in constant jammer), these jammers constantly transmits normal packets. It mislead other nodes to trust that a valid transmission is in place so that they remain in receiving states until the jammer is turned off or dies [9].

c. *Random jammer*- This jammer sporadically spread either arbitrary bits or normal packets into networks. It saves energy and toggles between sleep phase and jamming phase [9].

TABLE I
IMPORTANT FEATURES OF PROACTIVE JAMMERS

PROACTIVE JAMMER	TRANSMISSION OF BITS	ENERGY INEFFICIENT
Constant	Continuous, random bits	Yes
Deceptive	Continuous, regular bits	Yes
Random	Either random or regular	No

2) Reactive Jammer

Reactive jammer are different from proactive in terms unlike proactive, reactive initializes sending of jam signals when it sense that network is in active state. Therefore it requires being active every time and monitoring the channel. Hence it uses more energy than random jammer [9], [10].

a. *Reactive RTS/CTS jammer*- When the sender sends a RTS message, jammer senses it and jams the network. It then initializes the jamming results the receiver not to respond back as CTS reply due to the damage of RTS packet [10].

b. *Reactive Data/ACK jammer*- It alters these packet's transmission. In the first case, because the information packets are not received properly at the receiver, they have to be re-transmitted. While in other case, ACKs does not destined to the sender, it is assumed that something have has gone wrong at the target side, e.g. buffer overflow. Therefore, it requires sending the data again [10].

TABLE 2

IMPORTANT FEATURES OF REACTIVE JAMMERS

REACTIVE JAMMER	TRANSMISSION OF BITS	ENERGY INEFFICIENT
RTS/CTS jammer	During RTS/CTS sent	Yes
Data/ACK jammer	During Data/ACK sent	Yes

IV. PRACTICAL EXECUTION ON KALI USING WEBSPLOIT

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing [23]. I tried to jam the wireless network using Websploit in Kali. It disconnects all the targets and access points to which clients are connected. That means the client is disconnected on a window host and unable to connect again. This will continue in the situation until we impede the wifi jammer and close the aireplay-ng window. It also prevents novice and detached clients to get in contact with the Wi-Fi network connection.

Following command provides an overview of modules that are available. Select the Websploit Wi-Fi Jammer module:

Fig. 1 show modules

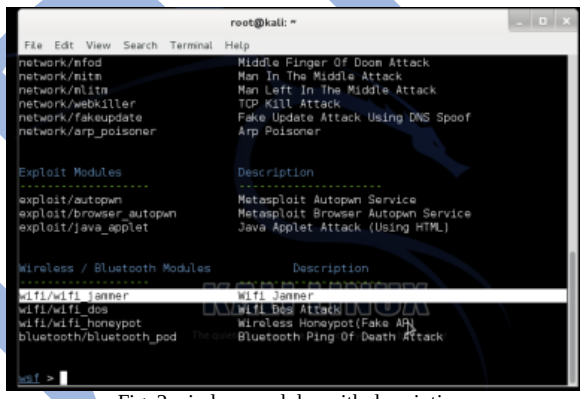

Fig. 2 wireless modules with description

From Wireless modules, opt for wifi/wifi_jammer module:

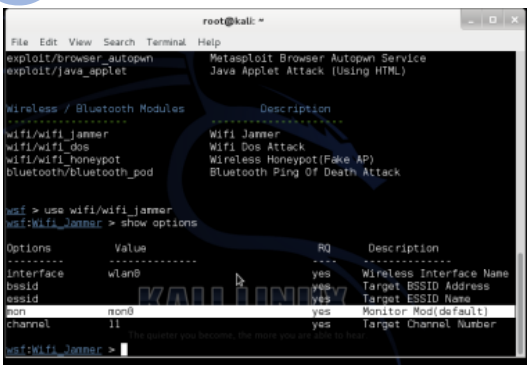

Fig. 3 use wifi/wifi_jammer

After locating the module, ask for showing the options and description. Using aircrack-ng, we can find the channel, BSSID and ESSID.

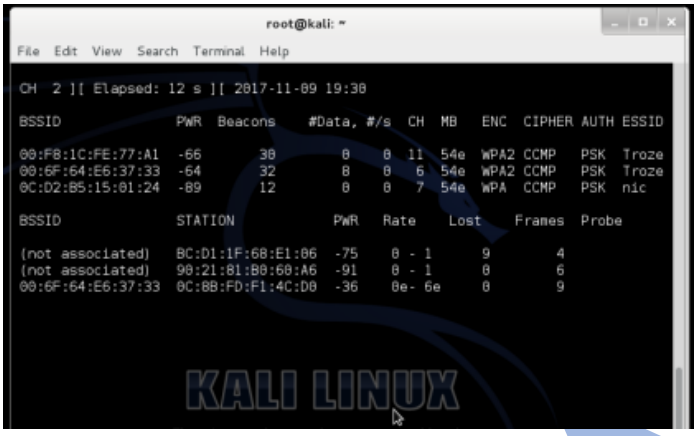

Fig 4 find channel, BSSID and ESSID

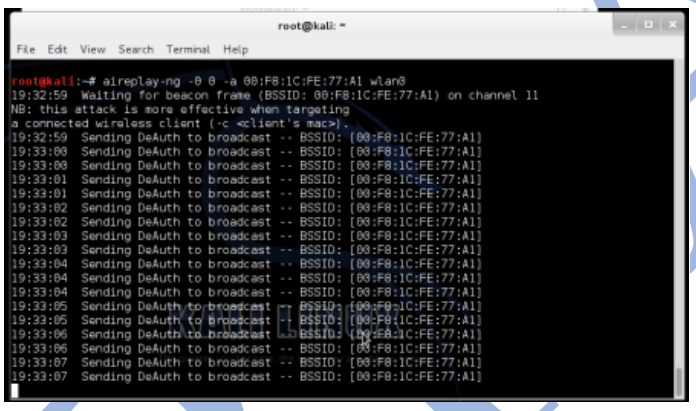

Fig. 5 detach the client from AP

It will detach the client from access point and targets automatically.

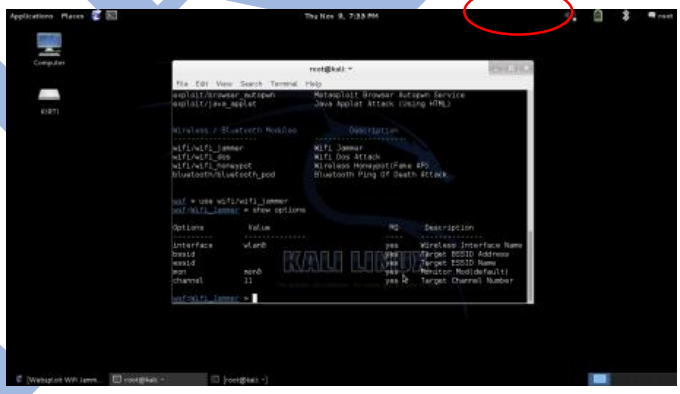

Fig. 6 Wifi jammed using Websploit

V. JAMMING DETECTION AND COUNTERMEASURE

When jamming is detected, jammed area can be mapped by the network nodes and re-route traffic, switch channel to thwart this jamming act. A comparative analysis is being shown in table 3.

A. *JAM: jammed-area mapping protocol*

It routes the packets around the exaggerated area. It can plot a wedged area within 1 – 5 seconds. As the value of node reaches below the threshold, system arises the information in the form of message either JAMMED or UNJAMMED and broadcasts it to the neighbors. When the announce timer expires, a BUILD message is send by the node that comprises of the group id. Upon receiving these messages, a message TEARDOWN is used by mapping nodes to notify the recovered nodes. After the achievement of the mapping process, all the nodes in the network get the message to reroute a path avoiding the area mapped as jammed.[11], [2].

B. Ant system

This is the system used to detect the jam at PHY layer and destined the messages to the target node. It formulates a hypothesis to test whether a DOS attack is genuine or not. There is an agent who traverses iteratively and gathers knowledgeable information about various routes to a target. They used following jammers: single-tone, multiple-tone, pulsed-noise, and Electronic Intelligence. The node detection is based on its availability of resources such as hops, energy, distance, packet loss, Signal to Noise Ratio, Bit Error Rate and PDR. After certain metric checks, a decision model is used that states if the jamming detection is true or not. If there is a case arises of jamming on a particular link, that link being excluded for the route to be followed and supplementary path is explored [12], [2].

C. Hybrid system

Hybrid system unite 3 techniques to defend: base station (BS) replication, base station evasion and multipath routing between base stations. The replication scheme implies replicated base stations. Evasion scheme defines spatial retreat of a BS. Multipath routing is there where numerous data routes between a node and a base station. With the technique of BS replication, if one or more BSs are jammed, the non-jammed BSs can provide the services to the network. The last technique requires that every node should have multiple paths to the base station so that if one path is jammed, other path can serve [13], [2].

D. Using PDR with consistency checks

The existence of jammers cannot be determined using single measurement efficiently. This system detects the jamming if all close nodes have low PDR values. If there is a node, having no neighbors, the PDR value will be low. The jamming effect is not considered for such nodes [9], [2].

E. Channel hopping

Channel hopping or toggling of channel from one to another is measured to be the most admired countermeasure to jamming. Proactive channel hopping is the simplest realization. In proactive channel hopping, the current communicating channel is altered after a definite interval of time. If the access wait time of channel goes beyond to a given threshold value, it is assumed that jamming has been occurred and there is need to switch the channel using a pre-defined strategy. In basic channel hopping, the channel is chose from unused channel's set. In deceptive scheme, the selection set includes the presently used as well as unused channels. In this case, if anonymous user might anyhow being able to get the history, he can track the channel selected for hopping and starts jamming the subsequent channel continuously. The substitute is pseudo random channel hopping scheme, which uses a pseudo number generation scheme to choose channels unfamiliar to jammers. After the packet delivery ratio (PDR) is computed for that channel, communication is switched back to the initial channel. When the present channel's performance (PDR) goes down from a threshold, toggle the communications to other channel having best PDR value [2], [14], [15], [16], [17].

F. Hermes node (hybrid DSSS and FHSS)

DSSS and FHSS are used to defend from jamming attacks. For signal transmission, DSSS provides wider bandwidth while FHSS offers meddling avoidance. A hybrid scheme, called Hermes node, is anticipated to deal with jamming attacks. The node of Hermes performs 1,000,000 hops per second (FHSS) to evade the jammers. DSSS is used to formulate the attacker sense the data signals as white noise, which averts the anonymous person to detect the communication radio band. Synchronization between nodes is important for Hermes node to work properly, which is achieved by the sink [18], [2].

G. DEEJAM (Defeating Energy-Efficient Jamming)

This method was proposed by Wood et al. [19] DEEJAM, a fresh approach to defeat jammers. This is basically used to conceal messages from attacker, dodge its exploration and trim down the impact of corrupted messages. This result in a novel protocol, allowing network nodes to function effectively even in the existence of a jammer. These works contributed to define, implement and evaluate four classes of jamming attacks namely scan, pulse, activity and interrupt jamming [3], [19].

H. EMMAC (Energy-Efficient MAC)

This method was proposed by Tang, Lei, et al. [20] EM-MAC augments the employment of wireless channel. It resists the intervention and jamming in wireless by facilitating every node to animatedly optimize the selection of wireless channels it utilizes based on the conduit setting it senses [20], [3].

I. JAM-BUSTER

Jam-Buster, a jam-resistant protocol proposed to stomp out the isolation between packets by using three factors mainly equal sizes, randomize the wakeup times and implements multiblock payloads. These three techniques are

combined to cope with an intelligent jammer and force it to spend more energy to be effective. Authors evaluated energy consumption only on jammer's side whereas the lifetime of legitimate nodes was not considered. Since this system acts like proactive defense against a jammer, it should also permits the other MAC constraints such as overhearing, idle listening and end-to-end delay communication [21], [3].

J. SAD-SJ

SAD-SJ, a self-adaptive and decentralized MAC-layer, an approach in opposition to discriminating jamming in TDMA-based WSNs. SAD-SJ is based on a arbitrary slot reallocation where each node achieves a arbitrary permutation of slots. The permutation process can be done after generating a random number. The protocol was proved to be self-adaptive in that it allowed nodes to freely join and leave yet keeping security of other nodes intact. It does not reduce performance and the additional energy consumed is insignificant [22], [3].

TABLE 3
CLASSIFICATIONS OF JAMMING DETECTION AND COUNTERMEASURES

S.No	Techniques	Type	Proposed attack	Countermeasure
1	JAM	WSN	Maps out the lodged area in WSN and routes packets around the exaggerated area.	Number of unsuccessful attempts above 10, detects the presence of jammer.
2	ANT system	WSN	Physical layer jamming, redirects the message to a destined nodes.	When there is a case arises of jamming on a particular link, that link being excluded for the route to be followed and other route is explored.
3	Hybrid system	WSN	Base Station failure could lead to collect sensor readings and executes tasks for command and control.	BS replication. BS evasion. Multipath routing between BSs.
4	Consistency check	WSN	Necessitates enhanced detection schemes to remove ambiguity.	Low PDR + Consistency check.
5	Channel hopping	WSN/WLAN	Constrained orthogonal channel's number and frequency separation is small between channels. If somehow anonymous person get the information about the history, he can track the channel and jam the subsequent channel continuously.	This frequency hopping is effective only when the number of orthogonal channels is large. Use "pseudo random channel hopping scheme" which selects channels unidentified to jammer based on a PN generation.
6	Hermes node	WSN	Node network interferes the radio frequencies using powerful jamming source and disrupts the WSNs function.	A secret word is used as a seed for the generation of PN code and channel sequence. This secret word is hard coded so that entrance of new node in the network can be detected with the existing nodes.
7	DEEJAM	LR-WPANs	Internet jamming. Activity jamming. Scan jamming. Pulse jamming.	Hide messages from attacker, dodge its exploration and trim down the impact of degraded message.
8	EM-MAC	WSN	Continuous jamming.	Avoid jammer channel selection.
9	JAM-BUSTER	WSN	Schedule prediction.	Proactive defense against a jammer.
10	SAD-SJ	TDMA based WSN	Transmitting malicious signal during slots of frame.	Random permutation of slot timers.

VI. CONCLUSION

Multi layer Jamming attacks are considered a precarious threat since they may become the origin to severe DoS, especially in the case when the attacker is intelligent. Till now, there is no such anti-jamming technique has been implemented that can be applied to all kinds of jammers. The main research focus is primarily on energy efficiency. In summary, as the jamming is being sensed in the network, nodes either toggle to non-jammed channel

or simply shifted to non-jammed area. Moreover, due to mobility of nodes, anti-jamming is extremely difficult in mobile networks and IEEE 802.11 networks.

REFERENCES

[1] Wikipedia contributors. "Internet of things." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 10 Nov. 2017. Web. 12 Nov. 2017.

[2] Grover, Kanika, Alvin Lim, and Qing Yang. "Jamming and anti–jamming techniques in wireless networks: a survey."International Journal of Ad Hoc and Ubiquitous Computing 17.4 (2014): 197-215.

[3] Hamza, Taieb, et al. "A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs." Vehicular Technology Conference (VTC-Fall), 2016 IEEE 84th. IEEE, 2016.

[4] Thakur, Neha, and Aruna Sankaralingam."Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks." Dept. of Software Engineering, SRM University, Chennai, India (2013).

[5] Anitha, K., and S. Usha. "A Scheduled Based MAC Protocols for Wireless Sensor Network: A Survey."

[6] Mpitziopoulos, Aristides, et al. "Defending wireless sensor networks from jamming attacks." Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on. IEEE, 2007.

[7] Kim, Yu Seung, and Heejo Lee. "On classifying and evaluating the effect of jamming attacks." The 24th edition of the International Conference on information Networking (ICOIN). 2010.

[8] Law, Yee Wei, et al. "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols." ACM Transactions on Sensor Networks (TOSN) 5.1 (2009): 6.

[9] Xu, Wenyuan, et al. "The feasibility of launching and detecting jamming attacks in wireless networks." Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2005.

[10] Pelechrinis, Konstantinos, Marios Iliofotou, and Srikanth V. Krishnamurthy. "Denial of service attacks in wireless networks: The case of jammers." IEEE Communications Surveys & Tutorials 13.2 (2011): 245-257.

[11] Wood, Anthony D., John A. Stankovic, and Sang Hyuk Son. "JAM: A jammed-area mapping service for sensor networks." Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE. IEEE, 2003.

[12] Muraleedharan, Rajani, and Lisa Ann Osadciw. "Jamming attack detection and countermeasures in wireless sensor network using ant system." Wireless Sensing and Processing, proceedings of the SPIE 6248 (2006): 62480G.

[13] Jain, Sushil Kumar, and Kumkum Garg. "A hybrid model of defense techniques against base station jamming attack in wireless sensor networks." Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on. IEEE, 2009.

[14] Khattab, Sherif, Daniel Mosse, and Rami Melhem. "Jamming mitigation in multi-radio wireless networks: Reactive or proactive? "Proceedings of the 4th international conference on Security and privacy in communication netowrks. ACM, 2008.

[15] Khattab, Sherif, Daniel Mosse, and Rami Melhem. "Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks." Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[16] Wang, Huahui, et al. "Spectrally efficient jamming mitigation based on code-controlled frequency hopping." IEEE Transactions on Wireless Communications 10.3 (2011): 728-732.

[17] Yoon, S-U., et al. "Adaptive channel hopping for interference robust wireless sensor networks." Communications (ICC), 2010 IEEE International Conference on. IEEE, 2010.

[18] Mpitziopoulos, Aristides, et al. "Defending wireless sensor networks from jamming attacks." Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on. IEEE, 2007.

[19] Wood, Anthony D., John A. Stankovic, and Gang Zhou. "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks." Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on. IEEE, 2007.

[20] Tang, Lei, et al. "EM-MAC: a dynamic multichannel energy-efficient MAC protocol for wireless sensor networks." Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM, 2011.

[21] Ashraf, Farhana, Yih-Chun Hu, and Robin H. Kravets. "Bankrupting the jammer in WSN." Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on. IEEE, 2012.

[22] Tiloca, Marco, et al. "SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks."Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on. IEEE, 2013.

[23] Wikipedia contributors. "Kali Linux." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 9 Nov. 2017. Web. 13 Nov. 2017.

