IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 10, October. 2019, Series -IV, PP 06-13

Survey paper on variousWireless Networks Methodologies and Security Issues

B Vysageetha
Assistant Professor, Department of Computer Science and Engineering, Dr B R Ambedkar University College of Engineering, Etcherla, Srikakulam, A.P, India.
Received 16 October 2019; Accepted 31 October 2019

Abstract: The major goal of the paper is to show various kinds of Security attacks, their belongings and barrier classifications in Wireless Network which is vulnerable to security attacks and dangers because of its attributes and impediments. Security attacks are recognized and characterized from alternate points of view for example in light of network layer in which the Attack happens, explicitly network layer shrewd security highlights and the network security fundamentals, in view of assailant area, in light of transmission of data, in view of various convention stack layers and so on and the distinctive safety efforts that can be applied to safeguard against various attacks. This review paper centers around different parts of various security attacks, their belongings and protection instruments relating to each Attack and so forth. So this paper causes specialists to have an exceptionally solid thought regarding the security issues, existing attacks and they can likewise utilize the thoughts and ideas to assemble increasingly secure wireless network framework in future. A course can be acquired to grow new security systems to ensure new potential attacks alongside existing ones.

Keywords: Wireless Network, security, organized, unstructured, CIA, dynamic Attack, inactive Attack, convention stack.

I. INTRODUCTION

In Present, there is various growth of the development in advancements, for example, versatile registering devices, including workstations, individual computerized colleaguesand handheld computerized devices, has incited a progressive change in the figuring scene. Processing will currently depend on the capacity gave by the PCs, and the idea of all inclusive figuring develops and ends up one of the exploration hotspots in the software engineering society. The clients utilize the gadget and utilize the data anyplace they need to which has made it important to embrace wireless network as the interconnection strategy. It isn't workable for the all-inclusive devices to get wired network interface at whatever point and any place they have to associate with other all-inclusive devices in view of which analysts have settled on Wireless Network. A Wireless Network is an arrangement of wireless versatile nodes that progressively self-sort out in self-assertive and brief network topologies utilizing which individuals and vehicles can be internetworked in zones where requires wireless associations. In wireless network, nodes can legitimately speak with the various nodes inside their radio reaches; though nodes that not in the immediate correspondence range utilize middle of the road node(s) to speak with one another. Specially appointed devices fuse correspondence dependent on Wi-Fi which enable them to communicate with one another utilizing wireless (one jump) and versatile networks. Accordingly, any physical situation giving these correspondence administrations to individuals progressing turns into a potential coordinated effort field. Highlights of wireless Network: Unreliability of wireless connections between nodes. There is restricted vitality supply for the wireless nodes and the portability of the nodes, consequently the wireless connections between versatile nodes in the impromptu network are not reliable for the correspondence members. Continually evolving topology. Because of the persistent movement of nodes, the topology of the wireless Network changes continually. The nodes can ceaselessly move into and out of the radio scope of different nodes in the impromptu network and this causes changing directing data. Absence of joining of security: Due to the changing of topology of the specially appointed networks frequently, it is essential for each pair of contiguous nodes to fuse in the directing issue in order to anticipate some sort of potential attacks that attempt to utilize vulnerabilities in the statically designed steering convention. As a result of these highlights , the wireless Networks are progressively inclined to experience the ill effects of the noxious practices than the conventional wired network on account of which security issues should be dealt with the security issues for Wireless Ad Hoc Networks are troublesome than the ones for fixed networks. This is because of framework limitations in cell phones just as continuous topology changes in the Wireless networks. The framework limitations incorporate low-control, little memory and data transfer capacity, and low battery control. Everyone realizes that the center prerequisite for military applications managing trust and security! In other words,

security is the most significant issue for impromptu networks, particularly for those security delicate applications.

II. TAXONOMY OF WIRELESS NETWORKS

The distinctive element of wireless networks is that bundles (fragments) are transmitted with the nearness of wireless connections. A gadget can send messages in a wireless network through the wireless medium, air, to another gadget gave that the recipient is inside the transmission scope of the sender. This adds adaptability to how a wireless network is framed and organized. In addition, it underpins gadget versatility.

IEEE 802.11

IEEE 802.11 is a fundamental standard for Wireless Local Area Network (WLAN) correspondence. IEEE 802.11 standard was first presented in 1997. It was imagined for home and office conditions for wireless neighborhood and supports three kinds of transmission advances specifically

O Infrared (IR)

O Frequency Hopping Spread Spectrum (FHSS)

O Direct Sequence Spread Spectrum (DSSS)

In 1999 two other transmission innovations were incorporated Orthogonal Frequency Division Multiplexing (OFDM) and High Rate Direct Sequence Spread Spectrum (HR-DSSS). The second OFDM tweak plan was presented in 2001 for high information rates [2]. The standard presents two working methods of wireless networks, specifically, the framework networks and the specially appointed networks.

I) Infrastructured Networks

The foundation working mode (Fig 1) is a network with an Access Point (AP), in which all STAs must be related with an AP to get to the network. STAs speak with one another through the AP. An infrastructured one with arranged, perpetual network gadget establishments. It tends to be set up with a fixed topology, to which a wireless host can associate through a fixed point, known as a base station or a passage. The last is associated with the spine network, regularly through a wired connection. Cell networks [3] and a large portion of the wireless neighborhood (WLANs) [4] work as the static infrastructured networks. Every single wireless host inside the transmission inclusion of the base station can interface with it and use it to speak with the spine network. This implies all correspondences started from or bound to a wireless host need to go through the base station to which the host interfaces legitimately. What's more, an infra-organized network is additionally be built up with a semi static or a powerful topology. A satellite network [5] has a place with this classification. It has a domain portion and a ground section. The domain section involves satellites. The ground fragment has various base stations, otherwise called portal stations (GSs), through which all interchanges by means of whole deal satellite connections occur. The base station, or passage, is a basic component for correspondence.

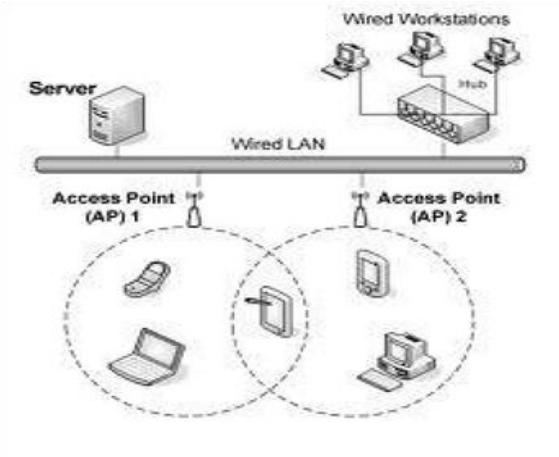

Fig. 1 Infrastructure wireless network

To keep up a progressing association when a portable host moves from the inclusion of its base station, a terminal handoff happens with the end goal that a versatile host hands over its intermediary for correspondence starting with one base station then onto the next one. At whatever point the inclusions of a few neighboring base stations cover with one another, a portable host may associate with one of the reachable base stations dependent on specific criteria.

ii). Specially appointed Networks

The second working mode, the free mode or the specially appointed mode (Fig 2) is utilized if there are no Access Points (APs) in the network. In this mode, Stations (STAs) structure an Ad hoc network straightforwardly with each other.An specially appointed network, for example, a bundle radio network, is one without a fixed topology. A wireless host can openly speak with another host straightforwardly at whatever point the collector is in its transmission inclusion. On the off chance that a wireless host might want to send messages to another host which isn't in the inclusion locale, it will first transfer them to a host in quite a while transmission go. The host capacities as a hand-off to advance the messages on its way to the goal. The significant bit of leeway of this arrangement is adaptability. An impromptu network can be assembled effectively, without the need of any preset, fixed framework. Moreover, a specially appointed network is commonly more strong than an infrastructured network as it doesn't have any basic gadget to keep up the network availability. At the end of the day, it is far-fetched a specially appointed network will be parceled because of the disappointment of a wireless host, however the glitch of a base station may segment a framework network, obstructing the correspondence between every single wireless host interfacing with the bombed base station and every single other host in the network. Nonetheless, there are a few disadvantages for specially appointed networks. To start with, it is significantly more troublesome and complex to perform steering in specially appointed networks in light of regular changes in the network topology because of host versatility.

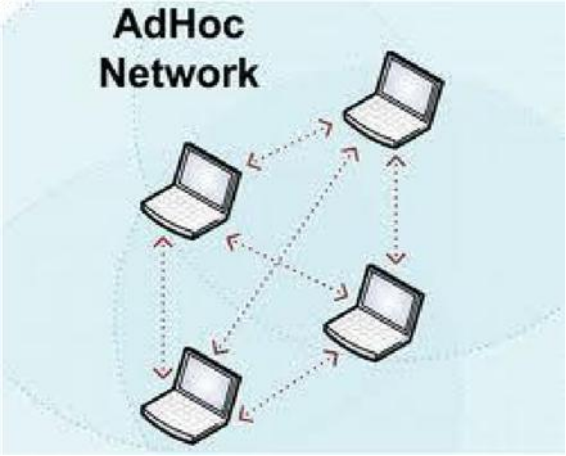

Fig. 2 Ad Hoc wireless network

Second, it is increasingly hard to control or arrange appropriate activity of an impromptu network, since every wireless host may have its own calculations to perform exercises, for example, time synchronization, control the board, and parcel planning. In an infra organized network, these calculations are regularly executed in and in this manner fit by the base stations or passageways.

III. WHAT IS WIRELESS NETWORKING?

Wireless networking alludes to the "usage of cross-merchant industry norms, for example, IEEE 802.11, where nodes convey without waiting be wired" (Mamoukaris and Economides 2003, p.1). The foundation of wireless networks utilizes standard conventions that are arranged by the requests of the network. This causes the limit just as the nature of administrations of wireless networks to change dependent on the devices. Wireless networks are ordinarily expected to manage devices that are produced using different fabricates. The networks are hence expected to have the option to help diverse equipment advancements, models, and transport conventions and furthermore control the progression of traffic inside the network.

Every wireless network utilize waves in the electromagnetic range extend. For instance, Wireless neighborhood (Wireless LANs) utilize high recurrence electromagnetic waves to transmit information. Balance and demodulation of the radio waves used to transmit information happens at the transmitter and recipient individually. They work in the business, logical, and restorative (ISM) radio groups and unlicensed-national data foundation (U-NII) groups (Zheng 2009). The networks are frequently associated with switches with the end goal for them to get to the web. Reynolds (2003) pronounces that Wi-Fi can possibly let anybody with a processing gadget to associate with the web at noteworthy paces without the need

Wireless networks likewise utilize the Open System Interconnect (OSI) reference model in the transmission of information. The way wherein this reference model applies to wireless networks is like wired networks with certain distinctions in the information connection layer where wireless networks arrange access by information to a typical air medium and furthermore manage mistakes which happen because of the inalienable idea of the wireless medium. At the Physical layer, the information is transmitted as radio waves.

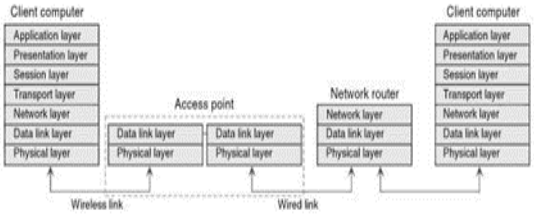

Fig 3: The OSI Protocol Stack and wireless correspondence

What we have to construct a Wireless Networking

Before a wireless network can be manufactured, it is imperative to run a site review. While this progression might be overlooked when executing a little wireless network, it is of outrageous significance when building an enormous wireless network. This is on the grounds that wireless networks work at a similar recurrence band utilized by other gear, for example, carport entryway openers and microwaves and maintaining a strategic distance from obstruction from such types of gear is significance if the objective of solid correspondence is to be accomplished by the wireless network. Ganesh and Pahlavan (2000) note that the biggest speculation cost in setting up a wireless network is the expense of the physical site area and this organization is a developmental procedure since the network may need to modify in order to help an expanding number of clients and fulfill the interest for expanded limit and better nature of administration. Huge networks ought to be worked in view of sensibility and unwavering quality since they may develop to a point where the network executive can't successfully oversee them.

There are various equipment and programming parts that are required in executing a wireless network. One essential equipment gadget is a passage which is the gadget connecting the wireless network to a wired LAN. Wi-Fi Alliance (2004) noticed that the passage is the gadget that transmits and gets the sign which are utilized for conveying between the processing devices in the network. Wireless passageways have changing limits and the size picked is reliant on the speed wanted in the network. The gadget ought to be put at a focal area and at a high vantage indicate all together maintain a strategic distance from impediments and guarantee that the same number of clients approach the network. There are various noteworthy components that one needs to think about when procuring the equipment for the wireless network. Interoperability of the gear is a significant factor if the network is to help all the accessible conventions, (for example, 802.11a/b/g). The range which the network is required to length is additionally a significant thought. Details, for example, the transmission control and the recieving wire increase ought to be utilized to figure the scope of the hardware.

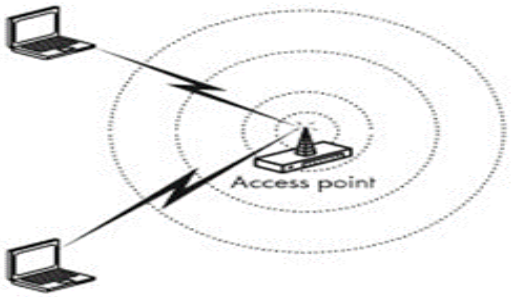

Fig 4: Access Point

Much of the time, wireless networks are likewise associated with the web. A switch which is a gadget that empowers a solitary web association with be shared by many registering devices on a similar network is material in such a situation. The range individual networking devices that can get to the wireless networks is extraordinary and it incorporates; PCs, individual advanced aides, tablet PCs, and pocket PCs. Every one of the devices getting to the network should be furnished with a working framework that takes into account correspondence over a wireless network. Wireless passages and the customer devices that are associated with them must be appropriately designed with the goal for them to work a TCP/IP network. The wireless customers to a network get their design subtleties from a DHCP which gives the devices their IP addresses, default portals, and subnet veils. In situations where the overseer wishes to enormously confine the clients, the IP locations might be credited physically. Such a move would clearly be work concentrated and unreasonable for a wireless network that serves a noteworthy number of clients.

IV. WIRELESS TECHNOLOGIES

There are a horde of wireless innovations and they contrast in the measure of data transmission they give just as the separation over which the nodes in the network can impart. Zheng (2009) sees that wireless advancements additionally contrast in the piece of the electromagnetic range that they use and the measure of intensity expended. To give physical availability, wireless network devices must work in a similar piece of the radio range and two wireless cards in this way should be designed to utilize a similar convention on a similar divert with the end goal for correspondence to happen. There are four noticeable wireless innovations which are; Bluetooth, WiFi, WiMAX and 3G cell wireless.

	Bluetooth 802.15.1	Wi-Fi 802.11	WiMAX 802.16	3G Cellular
Typical link length	10 m	100 m	10 km	Tens of km
Typical bandwidth	2.1 Mbps (shared)	54 Mbps (shared)	70 Mbps (shared)	384 + Kbps (per connection)
Typical use	Link a peripheral to a notebook computer	Link a notebook computer to a wired base	Link a building to a wired tower	Link a cell phone to a wired tower
Wired technology analogy	USB	Ethernet	Coaxial cable	DSL

Table 1: Popular Wireless Technologies

• Bluetooth

Bluetooth (IEEE 802.15.1) is the innovation that is utilized to embrace short-extend correspondence between note pad PCs, PDAs, cell phones and other individualized computing devices. The innovation is more advantageous than associating devices with a wire to impart. Bluetooth works in a permit free band at 2.45GHz and the correspondence range is about 10m and because of this short range, the innovation is sometimes classified as an individual region network (PAN) (Zheng 2009). A significant thought with Bluetooth innovation is control utilization and commonly, the innovation furnishes paces of up to 2.1Mbps with low power utilization.

• Wi-Fi

Wi-Fi represents wireless loyalty innovation and the term is ordinarily used to depict a wireless neighborhood dependent on the IEEE 802.11 arrangement of norms. The IEEE 802.11 measures settle similarity issues between producers of wireless networking gear by indicating an "over the air" interface comprising of "radio recurrence innovation to transmit and get information between a wireless customer and a base station just as among wireless customers discussing legitimately with one another" (Reynolds 2003, p.3).

Wi-Fi portrays a group of radio conventions which incorporate 802.11a, 802.11b, and 802.11g. 802.11b is the most well-known wireless networking convention being used and it utilizes a regulation called Direct Sequence Spread Spectrum in a bit of the ISM band from 2.412 to 2.484GHz (Zheng 2009). The most extreme speed offered by this convention is 11Mbps with usable throughput of up to 5Mbps. 802.11a is a convention approved by the IEEE and it utilizes a balance plan called Orthogonal Frequency Division Multiplexing (OFDM) with a most extreme information pace of 54Mbps. It works in the ISM band somewhere in the range of 5.745 and 5.805GHz. The recurrence range utilized by this convention is moderately unused which makes obstruction uncommon. In any case, Zheng (2009) noticed that utilizing this part of the range is unlawful in many nations including the USA. 802.11g is rapidly turning into the "de factor standard wireless networking convention and it is turning into a standard element for workstations and a ton of hand held devices" (Singh 2009 p.56). The convention utilizes the ISM band from 2.412 to 2.484GHz (same as 802.11b) however it uses the OFDM regulation plan. The most extreme information rate for 802.11g is 54Mbps and it is in reverse good with the well-known 802.11b convention.

• Wi-MAX

A prominent type of broadband wireless access for quick neighborhood association with the network is WiMAX. WiMAX is the condensing for Worldwide Interoperability for Microwave Access and it was institutionalized as IEEE 802.16 (Zheng 2009). WiMAX innovation has a regular scope of 1-6 miles yet the innovation can traverse a limit of 30miles which has made the innovation named a MAN. This determination has increased incredible achievement in the arrangement of web access and broadband administrations through wireless correspondence frameworks. WiMAX has a high limit which makes it productive in information transmission with rates of up to 70Mbps being given to a solitary endorser station. The first WiMAX physical layer convention is intended to spread sign at a recurrence of 10-66 GHz and the innovation can give both observable pathway inclusion and ideal non viewable pathway inclusion also.

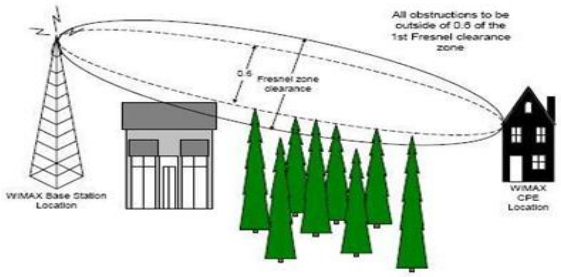

Fig 5: LOS Signal Transmission

The segments of a WiMAX incorporate; a Base Station, Subscriber Station, Mobile Subscriber and a Relay Station. The Base station associates and oversees access by the devices in the network. This part is comprised of numerous radio wires pointed in various ways and handsets which are essential for the wireless information network correspondence. A supporter station is a fixed wireless node which speaks with the base station and structures a connection between networks. A portable supporter is a wireless node that gets or transmits information through the Base Station while the transfer station is a Subscriber Station whose reason for existing is to retransmit traffic to the hand-off stations or endorser stations. A huge value of WiMAX is that it bolsters high versatility by client devices. A client can get to the network inasmuch as they don't surpass the edge speed which is typically esteemed at 120km/H. This property of the innovation takes into consideration conveyability since the client can cross a critical zone which is secured by various base stations without interfering with their present session.

• Cellular Networks

While cell phones have increased overpowering conspicuousness in the previous decades, cell phone networks were presented as far back as the mid 1980s and this innovation had the option to give access to the wired telephone network to versatile client (Kumar and Manjunath 2008). The region of inclusion by the cell wireless network can run from a couple of hundred meters to a couple of kilometers in sweep. In every cell, there is a base station which is associated with the wired network and which permits the cell phones in the range to speak with one another.

Fig 6: Cellular Transmission Towers.

As of not long ago, cell networks were driven essentially by the need to give voice communication (Kumar and Manjunath 2008). Be that as it may, with the development of interest for versatile web access, there emerged a need to give packetized information access on these networks also. While portable networks were created with the essential target of giving wireless access to voice administrations for versatile clients, the development of the web as the true network for data scattering has made web get to a necessary prerequisite in many nations. This need has powered the advancement of versatile networks and the development of Mobile Cellular Networks is grouped in ages from 1 to 4. The First Generation framework was Analog in nature and it was utilized for the transmission of discourse administrations. Because of its constraints just as absence of interoperability between nations, second era (2G) portable frameworks were presented and these frameworks bolstered information move abilities though at extremely low piece rates (Kumar 2010). Attributable to the requirement for expanded information rate, the third era was conveyed and these frameworks had a high information limit. 3G innovation is fit for conveyance download rates of up to 14.4Mbps in this way fulfilling the needs for high information speeds by customers. Cell gauges are expensive to the client since cell's utilization authorized range which are claimed by phone administrators. Forward Generation portable framework is the most recent innovation that is as yet being created. This innovation will have expanded limit and it will attempt to "incorporate all the portable advances that exist (for example GSM, GPRS,

Universal Mobile Communications, Wi-Fi, and Bluetooth)" in order to blend the numerous administrations gave and subsequently upgrade client experience (Kumar 2010, p.70).

Bit of leeway of Wireless over Wire Technology

Wireless networks have various critical points of interest over wired networks. In the first place, it is moderately simpler to set up a wireless network framework that it is to make a wired one. This is on the grounds that the physical devices vital for wireless networks are less that for wired networks. In introducing a wired network, one would need to spread out the links to interface the devices and this procedure isn't just costly yet in addition work and time escalated. Wireless networks require a passage and one different devices have been appropriately designed they can work. Another extra value of wireless networks is that development of a current network is simple since availability is now accessible inside the scope of the passageway. The simplicity of sending of wireless networks makes them financially alluring for most associations since the capital speculation of actualizing these networks isn't as scary that that required for expand wired networks. With the wide achievement of wired LANs, the neighborhood registering business sector has made a consistent move towards wireless LANs which offer indistinguishable rates from wired LANs.

The versatility of wireless networks is another credit that charms them to clients. Wireless networks are worked with the thought that most clients who need to get to information will be versatile and wired associations may in this manner demonstrate to be a significant burden. With wireless networks, an individual will stay associated as long as they are in inside the scope of an Access Point. All things considered, versatility isn't constantly a necessity for WLANs particularly in indoor business settings where the clients might be limited to one physical area throughout the day.

Fifteen years prior, wireless networks were for the most part constrained to huge organizations and government offices which could bear the cost of the restrictive expense of wireless foundation just as workstations. Notwithstanding, the expense of wireless networks has decreased fundamentally which has helped in the development of wireless LANS. Today is progressively efficient to put resources into a wireless network framework than it is to set up a wired network which implies that more people and associations are picking wireless networks.

• Demerits

Regardless of the focal points that wireless networks have, there are some significant hindrances which make it important to utilize wired networks in certain examples. In the first place, wireless networks are increasingly powerless to impedance when contrasted with wired networks. Wireless networks utilize radio frequencies and at some random time, there are radio obstructions in the air. The most consent utilized standard by numerous WLAN's is the IEEE 802.11b which is an unlicensed radio range that is shared by numerous customer devices. These devices which may incorporate cordless telephones and child screens work in a similar territory that most wireless networks are set up. Impedances subsequently happen when wireless specialized devices need to impart frequencies to shopper devices along these lines decreasing the viability of the network.

V. Various Types of Attack on Wireless Network

Classes of Attack may incorporate detached observing of interchanges, dynamic network attacks, close-in attacks, abuse by insiders, and attacks through the specialist co-op. Data frameworks and networks offer alluring targets and ought to be impervious to Attack from the full scope of risk specialists, from programmers to country states. A framework must have the option to constrain harm and recuperate quickly when attacks happen.

There are five sorts of Attacks:

Passive Attack

A PassiveAttack screens decoded traffic and searches for clear-content passwords and delicate data that can be utilized in different kinds of attacks. Uninvolved attacks incorporate traffic investigation, observing of unprotected interchanges, decoding feebly encoded traffic, and catching confirmation data, for example, passwords. Latent interference of network tasks empowers foes to see up and coming activities. Aloof attacks bring about the revelation of data or information documents to an aggressor without the assent or learning of the client.

Active Attack

InActive Attack, the aggressor attempts to sidestep or break into verified frameworks. This should be possible through stealth, infections, worms, or Trojan steeds. Dynamic Attacks incorporate endeavors to evade or break assurance highlights, to present malevolent code, and to take or alter data. These Attacks are mounted against a network spine, misuse data in travel, electronically enter an enclave, or Attack an approved remote client during an endeavor to associate with an enclave. Dynamic Attacks bring about the revelation or dispersal of information records, DoS, or adjustment of information.

Distributed Attack

ADistributed Attack necessitates that the enemy present code, for example, a Trojan steed or indirect access program, to a "trusted" part or programming that will later be circulated to numerous different organizations and clients Distribution Attacks center around the malevolent change of equipment or programming at the industrial facility or during dispersion. These Attacks present vindictive code, for example, an indirect access to an item to increase unapproved access to data or to a framework work sometime in the future.

Insider Attack

An insider Attack includes somebody from within, for example, a disappointed worker, Attacking the network Insider Attacks can be malevolent or no malignant. Malevolent insiders deliberately spy, take, or harm data; use data in a false way; or deny access to other approved clients. No pernicious Attacks commonly result from heedlessness, absence of learning, or deliberate circumvention of security for such reasons as playing out an errand.

Close-in Attack

A nearby in Attack includes somebody endeavoring to get physically near network parts, information, and frameworks so as to get familiar with a network Close-in Attacks comprise of normal people achieving close physical nearness to networks, frameworks, or offices to alter, assembling, or denying access to data. Close physical vicinity is accomplished through secret section into the network, open access, or both.

VI. CONCLUSION

This paper represents the different research issues and difficulties in the wireless domain, scientific classification of wireless network, diagram of a thorough rundown of research issues and difficulties of the wireless network like sign blurring issue, portability issue, power and vitality, information rate improvement, security and the nature of administration issues of the wireless networks. What's more the prevalence of wireless networks developing at an exponential rate, the information rate upgrades, limiting size, cost, low power networking, client security and the best necessity to acquire the required QoS issues turns out to be all the more testing since wireless networks are quickly getting to be well known, and client interest for valuable wireless applications is expanding. From all the accessible conveyed and brought together frameworks, four most normally utilized dispersed frameworks were examined top to bottom and after that the security issues looked by these frameworks and the arrangements proposed by different scientists were talked about inside and out. At long last the security issues and arrangements proposed for various frameworks were condensed and contrasted and one another. Security is an extremely perplexing point.

REFERENCES

[1]. S. Misra, I. Woungang and S. C. Misra, “Guide toWireless Networks”, c Springer-Verlag London Limited, pp. 1, 2009

[2]. J. Zheng and A. Jamalipour, “Wireless Networks A Networking Perspective”, A John Wiley & Sons, Inc., Publication, pp. xxiii-2, 2009

[3]. C. S. Raghavendra, K. M. Sivalingam and T. Znati, “wireless networks”, Kluwer academic publishers New York, Boston, Dordrecht, London, Moscow, pp. xiv, 2004

[4]. M. U. Aftab, O. Ashraf, M. Irfan, M. Majid, A. Nisar and M. A. Habib, “A Review Study of Wireless Networks and Its methods:

[5]. Kavitha, T., and D. Sridharan, “Security vulnerabilities in wireless sensor networks: A survey”, Journal of information Assurance and Security 5.1 (2010): 31-44.

[6]. D. Singla, C. Diwaker, “Analysis of Security Attacks in Wireless Sensor Networks”, International Journal of Software and Web Sciences (IJSWS), ISSN (Print): 2279-0063, ISSN (Online): 2279-0071

[7]. Prabu, M., et al., “DOS Attacks and Defenses at the Network Layer in AD-HOC and Sensor Wireless Networks, Wireless AD-HOC Sensor Networks: A Short Survey”, Middle-East Journal of Scientific Research 23.5 (2015): 779-784.

[8]. Mohanty, Prabhudutta, et al., “SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY”, Journal of Theoretical & Applied Information Technology 13 (2010).

[9]. Dhara, Buch, and JinwalaDevesh., “Denial of Service Attacks in Wireless Sensor Networks”, NUiCone 2010. 2010.

[10]. Mohammadi, Shahriar, and HosseinJadidoleslamy, “A comparison of physical attacks on wireless sensor networks”, International Journal of Peer to Peer Networks 2.2 (2011): 24-42.

B Vysageetha." Survey paper on variousWireless Networks Methodologies and Security Issues." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 10, 2019, pp. 06-13