Journal of Theoretical and Applied Information Technology
15th July 2017. Vol.95. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

WIRELESS LOCAL AREA NETWORK: A COMPREHENSIVE REVIEW OF ATTACKS AND METRICS

[1]SAMIRA SARVARI, [2]NOR FAZLIDA MOHD SANI, [3]ZURINA MOHD HANAPI, [4]MOHD TAUFIK ABDULLAH

[1,2,3,4] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang Selangor, Malaysia

E-mail: [1]samirasarvari82@yahoo.com

ABSTRACT

Wireless Local Area Networks (WLAN) was once a single network solution. Yet now, it contributes to all part of business and computer industry. Thus, WLAN security measures need special attention. In order to identify WLAN networks' vulnerability, some intrusion detection systems, architecture, and potential threats in the literature of this area is investigated. This approach is to categorize present wireless intrusion detection system (IDS) and detection technique. Several advantageous and drawbacks are presented and an in-depth critical literature review is presented. Different WLAN attack types and review some metrics in relation to operability and performance of IDS is summarized and extensively argued which can be conducted through integrating both practitioners and scholars. The future research areas are also discussed.

Keywords: *Wireless Local Area Networks (WLAN), Intrusion Detection System (IDS), Network topology, Ad-hoc Network, Network attack*

1. INTRODUCTION

Although Intrusion detection has been extensively studied, but there is a need to be investigated by researchers critically, in order to help detection of malicious activities within a variety of promising software applications. Other than malicious activities prevention, intrusion detection can function as a useful instrument, to act as protection against unauthorized access to computer applications, particularly the ones with more sensitivity of faults in the real world. Moreover, the inhibition of unauthorized access to wireless networks is essential for people who maintain the wired networks, as well as for those who protect against any serious damage to wireless networks. Today, wired and wireless networks have been working together and a smooth connection was demonstrated between them, therefore it is crucial to understand how these networks can be running together. Any intruder can gain unauthorized access to the network by the assistance of unauthorized WAP (wireless access point). WLANs are dependent on IEEE 802.11 and they encompass many security defects [1, 2].

In the 1970s, TCP and IP protocols came into being having drawback such as flexibility [3]. Intrusion detection and intrusion prevention are utilized to protect any illegal access to WLAN data [4]. Even intrusion prevention proves inefficient against some intrusions. Intrusion detection searches for the opponents that have jumped over the network borderline. One method could be to find the nodes that possess anomalous background [5]. Pervious research endeavours can be classified as six IDS techniques classification in WLANs [6-9]. All these studies differ in four operational activities; detection technique, collection approach, multi-trust, and analysis approach. An in-depth overview of all above mentioned studies uncovered shining examples of the classification of WLAN IDSs:

- Anomaly detection technique encompasses Zhong Technique and Nodeprints [6, 7],
- Anomaly which integrated by signature detection system includes; MABDIDS, Haddadi, and Yuan Techniques [8, 10, 11],
- Signature includes Sneeze Technique [9].

From these researches it can be drawn that: The advantage of the study by Zhong et al. is finding that nominal features, instead of numerical features confuses results. The disadvantages of this study are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

marginal detection rates (65.3 to 82.5%) and strong assumptions [6]. Moreover, the anomaly based IDS in Mitchell research that relies on RSSI is one example of using raw multi-trust data to detect anomaly behaviours. The advantage of this study is that it improves performance by using multi-trust data from untrusted nodes [7]. The disadvantage of this study is that it does not accommodate mobility. Their approach focuses on spoofing attacks. In regard to signature-based design approach, the Sneeze algorithm to detect intruders on a WLAN and locate them have been proposed [9].Sneeze is essentially a signature based detection technique with a traffic based collection process and simple pattern matching. The authors focus on attacks involving a rogue access point/man in the middle. Hence, it is critical to find out the various types of wireless intrusions and the security standards to highlight the characteristics needed to further clear the concept. Complexity issues in elaborating IT projects will be present even when the most optimal development methodologies are used to achieve the specific goals [2], thereby, it can be asserted that categorization of present wireless intrusion detection system (IDS) and detection technique are of utmost important to meet the IT projects' mission [12]. Hence, it is critical to find out the various types of wireless intrusions and the security standards to highlight the characteristics needed to further clear the concept.

It was in this context that the author undertaken this research to introduce a crystalized the concept of intrusion detection, to classify the current IDS methodical approaches and last but not least to introduce the WLAN often concepts and the WALN intrusions often interpretations.

It is argued that this research endeavor contributes to theory and practice in three ways: First, incorporated and integrated an in-depth critical literature review; second, extensively discussed some measures to be taken against WLAN intrusion; Third, have provoked a debate about the significance of the topic in which can be conducted through integrating both practitioners and scholars. Also at the end of this study the future research areas have been discussed.

2. WIRELESS LOCAL AREA NETWORK (WLAN)

Wireless networks can be divided into two groups considering establishment and architecture of the networks: (1) infrastructure-based network and (2) ad-hoc (infrastructure- less) network. WLAN's Basic Model has been illustrated in Figure 1.

Figure 1: WLAN Basic Model

Furthermore, WLANs are giving the opportunity to their users for setting up a wireless communication within a range of 100 meters. WLANs can usually operate in different modes, either in infrastructure WLAN and ad-hoc mode or in infrastructure-based mode, or they can even function as an independent WLAN. An example of infrastructure mode WLAN is illustrated in Figure 2. Ethernet can connect the wireless stations to wired networks through WAPs. This would actually happen through WAPs in an infrastructure WLAN. Besides, in areas where network coverage is fully provided, wireless devices can move freely with no disruption.

2.1 Infrastructure-based Network

Fixed wireless access points (WAPs) in combination with a wired network have made up the Infrastructure-based wireless network. Thus, the data can pass on faster to the client devices on each side. End-users would use the clients' devices in order to have an access to network connection when they are not located in the static state. Currently, it has been shown that most of the devices' connections, which helps the users in mobility conditions, would occur over private networks, for instance, laptop users could have access to the Internet through WAPs. Two of the most commonly redistributed infrastructure wireless networks are known as (1) wireless local is a network and (2) cellular networks [4]. Some factors such as base stations, PSTN switches, mobile hosts and mobile switching centers can facilitate the construction of cellular network PSTN, connecting the base stations or fixed cell sites through MSC. Typically, an excellent coverage is granted by cellular networks and they are not limited, they also can enhance the capacity and provides diversified advantages over alternate solutions. The reason behind this is because a number of activities can be implemented at the base stations or the cell sites. Thus, the mobile or cellular communication networks are known as the building blocks for wireless wide area networks (WWANs), which are distributed throughout the land area.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2 Ad-hoc Network

As it has been depicted in figure 2, in independent WLAN or ad-hoc Network, nodes are capable of communicating with one another freely and they do not possess any fixed point. This has been proven to be convenient for people who use a laptop in public places for conducting a meeting. This has been acknowledged as an Independent Basic Service Set (IBSS) in IEEE 802.11 nomenclature [13]. The information can be exchanged through access points, by diversified loci in Independent Basic Service Set (IBSS) within themselves or other networks.

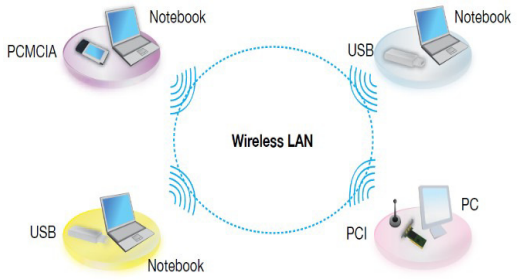

Figure 2: Ad-hoc Mode

If one of the nodes as an access point would be available for Independent Basic Service Set (IBSS), it can be considered as dependent and can be also marked as Basic Service Set (BSS). These access points are essential because every single information must be exchanged through them, which subsequently authorize these access nodes to safeguard the bundles and also to forward them in an enormous amount to the base functioning in short power organized manner. In infrastructure design, mobile nodes can exchange information through the steady access points. The network access points can be linked to wireless nodes with the wired nodes, in order to widen the ability of LANs. However, in some cases, services might extend to other areas where they can overlap with another one, and increase the possibility of bond development. Currently, this structure has been recognized to be identical to mobile networks throughout the world.

Infrastructure mode can be differentiated from an ad-hoc mode (A-Mode) based on different variables, such as the way the information is being communicated, as well as diverse other activities. In MAC frame header, FromDS and ToDS can be indicated clearly, whether the frame is being sent from the Distribution System or inside a Distribution System, respectively. In ad-hoc network, when any types of information exchange taking place, two of ToDS and FromDS bits together equal nothing. BSSID has recognized the Basic Service Set (BSSID) into which the frame was being transported. For differentiating the joint networks on the same pathway, it is important to know that BSSID is also tied in 802.11. MAC address of BSSID in infrastructure network has been referring to the wireless surface, which assists the BSS. BSSID has been chosen in an indefinite manner in ad-hoc network. The node has been connecting with a network by the intention of accepting the delivery of frames, which are having BSSID. Association ID has been also possessed by some of the frames being delivered to the access points (AP). In an Infrastructure mode, when a node is active, frames are generally being delivered to access points. In those types of situation, two bits of ToDS must be set to one and the other FromDS must be set up to zero. Moreover, the access points that MAC addresses, as BSSID must be accepted by frames. However, in comparison in A-mode, the frames with BSSID of an ad-hoc network as well as FromDS and ToDS set, nothing must be transmitted. In this paper, it has been demonstrated that nodes in ad-hoc network would be able to accept the frames, which has been sent by the access points properly [14].

2.3 WLAN security

The 802.11 is dependent on two verification techniques: Open authentication that does not require any verification and Shared Key authentication demands from the applicant to introduce a secret key for the authorization of access point. Presently, Wired Equivalent Privacy (WEP) is the security borderline for all 802.11 standards whose main aim is to protect WLANs just line wired networks. WEP is dependent on the RC4 symmetric algorithm. Administrators implement access keys on the access point and wireless gadgets which utilize the keys to encode and verify the completeness of information content. Besides this, the access points utilize the keys to verify its applicants. Even though the encryption power of RC4 algorithm is capable enough but the WEP standard follows the inefficient path in its utilization. One of the biggest afflictions possessed by wireless devices and their access points is that the secret keys are of shorter length than the secure protocols. WEP connects a shared secret key with a 24-bit initialization vector of short length to bring about 64-bit RC4 key stream. The initialization vector is forwarded to the receiver in plain text format so that the same key stream is being produced. This means that the intruders can notice

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the 24 bit IV being delivered through the utilization of WEP [15].

Also, the initialization vector could not be used for diversified messages because of not being big enough. An intruder can easily get access to the access protocol and the wireless devices by assembling initialization vector. Present 802.11 standard vendors no measurement for bringing any modifications initialization vector. Some merchants do utilize the initialization vector for IV stream. Some other systems produce the initialization vector in sequence to counter the breakdowns WEP security also lacks the proper explanation of key management. Because of this, the keys in the device could not be easily altered in case, the user loses its device then the intruder can utilize the key to compensate all the devices including the lost device. Active management of keys can help to enhance the complexity as well as turn off the warnings possessed by WEP keys descending in the incorrect direction [16].

3. TAXONOMY OF ATTACKS IN WLAN

Security is a primary concern for any network environment. The security in a network can be ensured via blocking intruders or attackers against gaining the access to network resources and network information. Network attackers are mostly attempting to make the network data unavailable to the users. Howard has been constructing an advanced anatomy, which could include the purpose of intrusions and its categories, hardware utilized, as well as invaders and an approach to sensitive content [17]. Howard taxonomy is presented in Figure 3.

Figure 3: Howard's Taxonomy of Attacks

Initially, the intruders try to take over the hardware or the device in order to execute an illegitimate act. Intruders can make use of different hardware devices to execute successful attacks to the network by looking for the vulnerabilities in the hardware devices or the network. Six of the most common types of attack categories are discussed as follows.

3.1 Network Discovery Attacks

Network Discovery attacks, which has been known as the materialized using tools that aids in the determination of the features of network including addressing of the merchant, MAC, information exchange route, security rules set in a network and SSID of the access point. Information extracted using such tools are later exploited for launching attacks on a network [18].

3.2 Eavesdropping/Traffic Analysis

Eavesdropping/Traffic Analysis, are popular attacks, which involves in listening to the private conversations. This attack allows the intruders to collect information and compose a descriptive analysis from wireless network [19]. Since the data inside 802.11 bundles are in the unencrypted format, it is easy for competent eavesdroppers to interpret them. One of the popular software that has been using for launching such attacks is "Air peek" [20].

3.3 Masquerading/Impersonation

Masquerading/Impersonation known as the attacks, which tries to abstract the identifications of genuine consumers or of authentic AP. The software is required for these attacks to modify the MAC address of the actual user address in order to duplicate the authorized user. The intrusion of this attack has been acknowledged as Rogue AP since it is capable of regulating the network traffic. Consequently, spying intrusion has become easy for intruders.

3.4 Man-In-The-Middle

In such attacks, the intruder is in the middle, that is, between the devices. Therefore, the intruder can make modification in the content as long as he has the encoded keys. Such as intrusion is not considered feasible in the network guarded by 802.11. This is due to the deployment of EAP techniques [21].

3.5 Daniel-Of-Service

These attacks have been attempting to hinder the usage of network information and any other resources to intended users. And has been causing more interruptions and absorbing costly network assets. It has been proven to be harmful to wireless networks because network restrictions can be easily endangered [22]. EAPOL-failure, WAPOL-start, EAPOL-Logoff and EAPOL-Success are some of the latest DoS attacks for 802.11i implementations. Because of the need of a solution for such attacks, DoS have become very important for wireless network administrators.

3.6 802.11i Oriented Attacks

In addition to 802.11i DoS attacks, in Transitional Security Network (TSN) some other hazardous threats have been founded, such as pre-RSNA and RSNA, which have been integrated, and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

permitted by 802.11i. Communication with both pre-RSNA and RSNA networks can be generated by user's gadget or any devices. In these type of situations, the opponent can, therefore, launch an attack in user's device by using pre-RSNA. The attack has been launched by unifying the frameworks from RSNA assembled Access points. A list of WLAN (802.11i) attacks is discussed in detail as follows.

Mac address spoofing: There is a difference between mac address spoofing and IP spoofing. Impersonation has been found to be more accurate in mac address spoofing because the invader does not use another source to build-up a data. Intruders would ensure about their wireless card right after resulting in any modification in their MAC address for sending and receiving purposes. Ipconfig tool or any other short length C program, which have SIOCSIFHWADDR flag, can be used in Modification of a mac address [20]. An intruder can achieve MAC address by Illegitimate access. Intruders can actually construct their MAC address with the purpose of deflect network intrusion detection systems (NIDS).

Bypassing access control lists: In order for granting permission to authorized MAC addresses for the purpose of exchanging information on the network, network administrators have been fixing the access points. These access control forms can be deflected by intruders, by regular base supervising network and producing only those MAC addresses that are allowed to exchange information [23].

Authenticated user impersonation: In this attack, intruders would closely observe the network functionality in order to be able to cross the security doorway. So, that subsequently they can gain access to applicants' authorized MAC address and following by that before exchanging information on the network create the applicants MAC address with the exact same characteristic. Because intrude has been possessing the potential to generate the dynamic list of MAC IDs, which do not resemble ID of association in any way. Noticing the MAC address can reveal such intrusions.

Deauthentication: Once 802.11 applicants have chosen the access point for the purpose of information exchange, it will authorize itself before any information exchange occur. The intruder would be able to have data access by acting either as an access point or applicant and then forward it to another one. However, no applicant or access points will be participating in the verification process, not until the process is set-up again [24].

Disassocation: Usually, there are no verified Association frameworks and 802.11 would control the de-authorized information. Abusing any vulnerable hole is similar to de-authentication or de-authorized intrusion. Importantly, the de-authentication intrusion has been identified to be more efficient than disassociation intrusion [25].

Address resolution protocol (ARP) poisoning has been created as a mediator between MAC and IP address in order to revolutionize the information content further, which includes handling the MAC and IP affair efficiently [26]. However, it has been reported that ARP data content could be tricked easily. An intruder can bring the modification in MAC to IP address from a distant place. This would result in changing the traffic direction and provoke modification in forwarding the accurate object to where ever the intruder desires.

Wormhole attack: In this intrusion, the intruders in a network would take reports the bundles at one spot or region, and continuously drift and transfer it to another network spot [27]. Wormhole intrusion has been identified to be unsafe and extremely dangerous to location based wireless security systems and ad-hoc network routing protocols and some trustworthy protocols have been introduced to address this intrusion issues [28].

Daniel of service attacks (DoS) can be experienced in several layers in OSI model. Intrusions, which did not allow the legal users to access networks have been produced in the wireless environment. Determination of the exact time and place that an intrusion should be performed was allowed by intruders due to lack of physical framework. The susceptible holes inside 802.11 MAC protocol have allowed the intruder to disorganize the network entirely, with less energy consumption by using some packet bundles [29].

Dictionary attack against PA: WPA has benefited from Pre-Shared Key, which has been protected as long as the key was secured. However, vocabulary intrusion can easily guess the poor-quality user identifications, which has been known as a user password. Moreover, it has been presented by intruders that the usage of packet insertion to verify handshake, logged off vocabulary intrusion could be launched and the Pre-Shared Key could be obtained to compose the WPA encryption. This has led to an illegal accessing of the network by the intruders. Particularly, the use of tricked MAC address has been making the identification of these intrusions very difficult. And the utilization

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

arbitrary key has been the quick fix against these types of intrusions.

Virtual carrier-sense attack has been known as the Network Allocation Vector (NAV) mechanism, which would be supported by the MAC layer. Huge bundle streams have been producing unassigned location places, possessing values of considerable duration along with RTS and CTS frames, host and ACK frames particularly bound for the access points [30].

Invalid state: Both associated and unauthenticated states have been impossible under standard 802.11. But they can be included through the utilization of 2-bit condition [6]. Some kind of intrusiveness might be the results of any type of unpractical attitude point.

Fragmentation attacks: IP has been divided into a number of bundles in Fragmentation attacks. If fragmented bundles in IPV4 gain an illegitimate access, there will be a chance that the appliance to which the bundles have been delivered might break down the IPV4 stack. This might happen while the application has been involved in the building of the crashed bundles. Corrugated portions can be handled in different ways by different types of operating systems [31].

Packet alternation can bring any types of changes in the bundle that is unidentified by the access points, which means that if an intruder is capable of detecting some of the data in bundles he can change it more and provoke it again in the network [32].

Packet re-routing has been allowed to altering the IP header in order to direct the bundles to the appliance on the wired network [32]. When the bundle has been delivered to the wired appliance, has exposed the data content, since it has been in an un-encoded form. TCP checksum has not been proved to be useful because it only has been inspected during its arrival to the target place.

Packet insertion: An attacker can insert the arbitrary packets into the network, by knowing a single plaintext message, since it has been given out the random stream linked to one of the IVs [34]. Therefore, in order to create malfunctioning of the network, attackers can insert synthesized packets into the system.

War driving: Any person with mobile devices would search for the Wi-Fi wireless network by extracting the network information [35]. Wireless networks have been facing this more than wired networks. Looking for the system security through a confined network is not wise. Thus, any kind of defects in the network security should be immediately reported.

Active Man-in-the-middle: Performing the MITM attack together with encoded HTTPS and SSH through the utilization of tools that have been security analyzed, is not difficult. The collaboration of most of the applicants with the access points having high signal has been discovered in the ESS organization. Applicants can be tricked by any crooked access point, by taking benefit of this attitude and come across with the node that has been executed the MITM attack in contrast to the delicate traffic [21].

High-power amplifiers: Enhancing the transmission rate to a large extent has been possible for the high potential amplifiers. Sending the bundles to a large distance area by an amplifier with either 1 or 8 watts, which further 802.1 lb. devices could collect has been possible. The vulnerability of bundles can result in disorganized services, for instance, the bundles that have been visible from the access points with which the applicant has exchanged the information content or the content has been passed from the applicant. High potential amplifiers would permit the intruders to penetrate the network access points if only the controlled antenna from a far-off distance has been utilized.

Multiple virtual access points: The attacker would be able to use a number of virtual access points in order to copy them and demand 802.1 lb. to connect with them. A diversified number of intrusions could have been launched against the applicant, once the linkage has appeared. MITM against HTTP and SSL web flow is one of the examples here. By transmitting access point flow of high potential, either of false IP settings a number of accesses points or fake SSID could be closed.

MAC ID based inference of access control list: Many access points have been refusing clients with a MAC ID, which could not be found in an access control list or another whitelist mechanism as a security feature. This has been unsuccessful against capable attackers, as they will be capable of inferring the set of valid MAC ID's associated with an active network, and subsequently assuming any one of these MAC ID's for their use as required.

4. INTRUSION DETECTION

An intrusion detection system has been known as a software device or application, which has been observing the activity of the network closely, in order to detect any malicious patterns or any types of security policies violation in the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

computing systems. Typically, intrusion detection systems have been consisted of stream sources, which gives an updated information regarding what is happenings, figuring out the existing threats and generating an alarm in a case where any kind of illegitimate activity has been detected, so that an immediate action can be taken. Wireless intrusions have been usually launched before any information content in present turn on wired networks. Therefore, it has been vital for the source to penetrate in the airwaves before the content has received on the access points [33]. The whole process has been depending on the present intrusion detection methods, which could have thus, possess more than one aspect. If the IDS produce an alarm without any threat being discovered, then the credibility of IDS can get deficient. Moreover, the IDS trustworthiness could also get curtailed if the threat has been presented but no alarm has been produced[34].

The precise outcome has been delivered by Signature-based techniques (Table 1) but has been showing some limitations against the historical intrusions [35-42]. Therefore, depending completely on the signature-based technique is not recommended until later when has been rectified. Sellers have been claiming to bring updated modifications to the recent intrusions within a short time period as well as changing the signature database within the applicant's premises. On the other hand, by careful observation of the network flow Anomaly-based detection (Table 2) has possessed the potential to reveal the hidden intrusions, however, they have been less efficient than signature-based [43-50]. Both signature and anomaly based techniques have been combined with each other in complex IDS techniques. The state analysis and policy deviation have been also included within the complex approach.

Table 1: Signature-based Technique and Associated IDSs.

Table 2: Anomaly based Technique and Associated IDSs.

Hybrid intrusion detection systems have been encompassed of signature and anomaly-based approaches. Two detection measurements have been possessed by the Hybrid method; one has been for detecting of familiar vulnerable infiltration using signs and the other one has been for network behavior auditing, for detection of any types of deviation from the usual network profile [51]. Any kind of attacks has been detected precisely by hybrid intrusion detection systems, however, this hybrid intrusion detection systems have been consuming more energy and other resources. Figure 4 presents the hybrid detection model of IDS [43]. Table 3 also represents the hybrid technique and associated IDSs [52-57].

Figure 4: Hybrid IDS

Table 3: Hybrid Technique and Associated IDSs.

The nodes in above model have been disconnected from one another and have classified into hexagonal areas similar to mobile or cellular networks. Cluster nodes have checked and controlled each of these areas, and regional nodes have been auditing cluster node. These regional nodes themselves have been controlled and authorized by base terminals, which have been arranged in the tree-like structure. Attack signatures have been accumulated in base terminals and moved towards the leaf nodes for detecting the malicious attacks. In the same vein, the method has possessed requirements of both irregular and regular actions. Anomaly detection has been done by measurement of any kind of divergence or change from the presented requirements. Authors did not observe any kind of detection ratio. Also, they did not highlight what kind of vulnerabilities would be detected by this method.

In addition, the misuse detection and support vector machine (SVM) have been utilized by hybrid IDS, which the mechanism includes Monitoring component, Analysis & detection and Alarm. Cluster-based Hybrid IDS mechanism is shown in figure 5. A well spread cultivated algorithm has been utilized to cultivate SVM in order to differentiate the fine and vengeful arrangements. An intrusion detection system has utilized stream flood and state evolution investigation to discover a sync flood attack, which has been introduced in [46]. The method has observed TCP in order to detect this types of attack arrangement, however, the mechanism has not been examined and applied yet. Cluster hybrid IDS has been shown in [47], the cluster head has possessed the charge for detection of intrusions with the main purpose of the reduction of the energy consumption. An improved IDS, which has been suggested in [48] was divided into signature-based detection, decision-making, and anomaly-based detection.

Additionally, Cluster-based Hybrid IDS mechanism is shown in figure 5. A well spread

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cultivated algorithm is utilized to cultivate SVM so as to differentiate between the fine and vengeful arrangements. This method of intrusion detection method is sketched in a way that it can function in clustered WSNs, where all nodes observe nearby nodes in their surroundings. An intrusion detection system that utilizes state evolution investigation and stream flood to discover sync-flood attacks has been introduced in [46]. Cluster hybrid IDS has been shown in Deng's research [47], the cluster head possesses the charge for the detection of intrusions with the main purpose of the reduction of the energy consumption an improved ID has been suggested in [48] divided into anomaly based detection, signature-based detection, and decision making.

Figure 5: Cluster-based Hybrid IDS

The network, which has been already managed was operated to recognize vengeful and bundles. Still another tree structured IDS has been having high effectiveness in the detection of security intrusions in the network layer, which was shown in [50]. In Table 4, a brief overview of some of these hybrid IDSs has been shown. Across OSI layers, separate requirements for the ideal solution have been changed with each other in another new security mechanism [58]. Conventional IDS can observe and detect attacks a single layer of the OSI model because they usually function in that specific layer. For example, it has been known that network layer IDS would be able to discover routing intrusions, however, they are not capable of acknowledging physical, MAC or transport layer deviations. With the ability to exchange information and other characteristics between separate layers, cross-layer IDSs have been having the potential to detect and discover attacks in diversified layers. This communication exchange has been taking place by using cross layer interface between separate layers. Even though a number of attacks in diversified layers have been discovered by cross-layer IDS, but this mechanism has been utilizing more computational assets and energy through proper examination and observation of parameters between layers. Cross-layer ID agent, which is CLIDA has been proposed in [59]. CLIDA has guaranteed that communication and information exchange would navigate all areas between MAC, network and physical layer. Cross-layer information component has been depicting information to all layers. The potential to discover intrusions in diversified layers has been possessed by CLIDA, the intrusion detection agent. Intrusions with good efficiency can be detected by architecture. Another cross-layer security technique has been proposed in [60]. It has been discovered that the proposed technique would consume the constrained assets of sensor nodes. Later in another study [61], intrusion track back technique and cross-layer security technique, which has been discovering flood was introduced. Different requirements from network and MAC layers have been utilized to discover diversified flooding intrusions. Description of low, medium and high intrusions has been recorded. Table 4 introduces contrasting IDs.

Table 4: A Comparison among IDSs.

4.1 multi-Dimensional Intrusion Detection For Wlan

Wireless LANs have been more harmful than their wired analogs. For network protection, the standard wire line attack discovery mechanism has not enough. The 802.11b protocol has been also susceptible to intrusions. Since vulnerable attacks on a wireless local area network could not have been discovered by any single mechanism, therefore, it has been vital to opt a multidimensional approach. Diversified attack discovery models, which have merged analytical and computable metrics that particularly is in association with two OSI two layers, was accommodated by efficient multi-dimensional attack discovery approach. In addition, they have merged anomalous approaches (Policy Deviations) and the efficient and effective borderlines. The computational mechanism has been including policy deviation Stateful Protocol Analysis (SPA) and Signature-based Detection (SD). Signature recognition has been examining bundles to look for diagrams resembling those present in the signature database matching anti-virus software. A proper guideline has been set and followed, in order to describe the satisfactory borderlines for the network functioning, effectiveness, and efficiency. For instance, possibly due to the abnormal allocation of the arranged access points, policy deviation investigation has produced an alarm. Those intrusions with WLAN protocols violation must take a proper investigation of a protocol specification to ensure that the protocol, which was utilized in WLANs have not been endangered. Undoubtedly, Anomaly-based detection or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

analytical analysis would be able to identify any kind of abnormal activity from the fine arrangement. Attributes of anomaly and misuse detection can be reviewed in a various way because there are no major differences between them. In one study, Stavroulakis and Stamp (2010) have introduced an arrangement to separate the biological ideas, computation-depended approach and artificial intelligence. This arrangement, however, has made it difficult to understand the detection approach features. Even though many shortcomings have been identified in explanation of detection approaches, but studies have introduced the categorization of understudy classes with a detailed explanation of their categories such as: State and Heuristic based, Pattern based, Statistics based and Rule-based. Table 6 presents the Intrusion Detection approaches, which have been organized. From Table 6, it can be also demonstrated whether the aspects of time series have been taking into consideration or not. With the proper approach, which has been introduced in the discovery of intrusion areas, such kinds of intrusions can be recognized. Performance area has mentioned the capabilities at which the IDS process flow analyzes the events [35]. The flow has been carefully detected by Signature-based detection and then it has searched the patterns physically arrangement against the signatures present in the database. By learning based examination of arrangement [62], this also can be done in an automated manner. Physical signature detection as an anti-virus system has been performing in a similar manner. Here the signature database amends in an automated manner as fresh signatures have been detected. On the other hand, automated signature learning systems need through erosion of complicated network functions and the remarkable data mining that can have an impact on the efficiency as well as effectiveness. The signature process must be capable of forwarding frames before being backed on the wire, in order to be more capable and efficient in tackling these intrusions [63]. Moreover, security guidelines have been given the description regarding the sufficient performance guidelines and network functioning [64]. A policy deviation engine would produce alarms if the earlier set performance borderline gets infringed and supports the Wireless LAN pattern [65]. Table 5 is also illustrated from these references [66-73].

Table 5: Advantages of IDS for WLAN and Ad-hoc Networks.

Table 6: Intrusion Detection System Classification in WLAN.

For instance, network and security administrator have been facing difficulties with rogue Access points. Because the workers have possessed the potential to buy and redistribute wireless LAN, it has been hard to realize when and where they have been redistributed unless the site has been physically scrutinized with a scanner. As soon as rogue access points have been deployed, a policy deviation engines should generate an alarm if the bluff access points get redistributed. For a well-performed wireless LAN, policy deviation engine requires an entry to wireless casing information from airwaves. Protocol analysis (SP) has been observing 802.11 MAC protocols from the abnormal behavior if being traced from the standards. Improved network and intrusion detection have been provided by proper in time observation [74]. Two of the examples of protocol intrusions have been including session DoS intrusions and hijacking. In order to discover the intrusion, which divides the protocol requirements, it has been essential to observe the condition. Certainly, un-doubtfully statistical anomaly detection, which was based on classical measurements, could have been classified as the discovery of anomalous network activity. By grouping and introducing the functions that lead to the fine measurement of activities, the basic standard network functioning has been described [75]. Considering the remarkable fine activity as the basic standard, deviations from normal behavior could have been detected by other mechanisms, which detect attacks.

How the intrusion detection mechanism has been differing from others was dependent on the surroundings. So far, IDS mechanism has been established for CPSs, WPANs, WLANs, WMNs and cellular networks WSNs.

4.2 Advantages And Disadvantage Of Ids Techniques

Table 7 and 8 elaborate the advantages and the disadvantages of IDS mechanism for administering WLAN and hock systems. TheSsignature based approach has been able to provide assistance to WLAN systems because they have had a clear performance and amendment of intrusion vocabulary. WLAN has possessed higher abilities, in order to distinguish WLAN from other

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cellular and WSN networks. ad-hoc networks have been also able to get assistance from signature-based approach because of its higher processing abilities. Anomaly based approach has been able to provide assistance to ad-hoc and WLANs networks due to its potential in discovering the hidden intrusions. The reputation-based approach has been also providing assistance to WLAN ad-hoc network in order to conclude mean nodes, particularly those applications, which have been unacceptable and the confirmation on mean nodes has been well explained. A number of behavior-based approaches, because of their minimal memory burden have been providing assistance to ad-hoc and WLAN networks; the alternative, a traffic based approach and requires a lot of storage. Traffic based approaches have been also able to provide assistance to ad-hoc and WLAN networks because of their data possesses characteristics have not been accessible to applications like SNR and RSSI. Assistance can be also provided to ad-hoc and WLAN by Multi-trust based approach networks, where the community has not been static. This is because the determined evidence has been providing a clear view of the system even when that data was prejudiced with unreliable input [7]. The signature-based approach has not been accepted easily and it has been facing some objections. Since these could have considered a huge intrusion vocabulary, applications, WLAN and ad-hoc network have been trying hard to keep the intrusion vocabularies clean for signature-based approaches. Anomaly based approaches have been also not accepted easily because of their poor detection rate. A clear idea of functionality was not possessed by ad-hoc and WLAN network applications and the deviation from normal behavior have not been agreed with the basic standard activity. WLAN and network ad-hoc applications have been also introducing threats to the specification-based approaches or requirement because experienced people have been usually trying hard to distribute the requirements for application without clear use cases. Even though they have not been using clear use cases, but examination and scrutinization from specification-based approaches have been required, which proves to be expensive to deliver requirements for these applications.

Table 7: Disadvantages of IDS for WLAN and Ad-hoc Networks

Reputation-based approaches also have not been accepted easily because they have been pointing out more towards the mean nodes rather than poor nodes. Even though they were not possessing any activity demanding and economic and responsibilities, but ad-hoc and WLAN network applications have been trying hard to take charge of the authorization of better but mean nodes. Because their portrait cannot be expressed in advance WLAN and ad-hoc network applications introduce some threats for behavior-based approaches [7]. Because of the varying clarity of the varying environment, WLAN and ad-hoc network applications have been trying hard with traffic based approaches to utilize the multitrust. Due to the productive community, which has proved problematic for the formation of reliable connections, ad-hoc and WLAN network applications have been also introducing threats to multi-trust based approaches.

5. IDS METRICS FOR WLAN

IDS has been utilizing the significant characteristics, which were used to design or implement the wireless intrusions on the network. SSID has been one among those measurements modeled, which has been allowing the convenient WLAN to guarantee that the wireless nodes have established a connection with the correct system. Network connection to the system would not be allowed if the SSID's do not resemble. For instance, WLAN in ABC University, which has been utilizing the ABCU as SSID. SSID must not be a component of airwaves; meantime, it also should not be revealed to the listeners. Similarly, BSSID and ESSID have well recognized the access points. Certain features have also portrayed a considerable character for protecting intrusions. Agile receivers have been also assisting in raising the wireless communication in different aspects and they restricted the torrent waves. It has been stated that it is much better to not leave the network open if there is no need for use of network in the nighttime. Verification of the crooked access points has been also important for security reasons. In the same way, in has been stated that default SSID ought not to be considered in the access point and it should be avoided since the intruders have been capable of gaining illegal access to it. Knowing the applicant's address by access point has been stated to be important before the linkage permitted. Permission must be granted to the administrators by access points in order to construct a sheet, which includes all MAC addresses of the applicants permitted by WLAN. It has been important to note that permission can only be granted to the cellular nodes. Besides this, 802.11 frameworks have

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

possessed the capability of recording the allotted microseconds. This has also computed the Network Allocation Vector (NAV) on every single node. Network Allocation Vector (NAV) would be permitted to broadcast further, the only *f* it approaches to point 0.

Table 8: Classification of Relevant Metrics for WLAN Attacks

This characteristic feature has been utilized by RTS or request to send and CTS or clear to send that coordinates admission to the pathway where an invisible base may be intruding the broadcast. When this exchange has been taking place, the transmitting node, in the beginning, has delivered a tiny sized RTS framework, which has possessed considerable time to finish CTS and data frame, RTS/CTS framework and some others. The targeted node has answered back to CTS and RTS having a freshly assigned time period. Therefore, CTS/RTS frames have been also presenting in the IDS measurements. Distributed Coordination Function Inter-Frame Space and Short Inter-Frame Space have been the two-time windows out of four-time windows, which were given preferences to enter the midway radio. It is the responsibility of the delivering frame to monitor a silent midway before any frame has been delivered at least for one of the represented windows. SIFS window has employed for frames, which have been delivered by a sector of enduring trade channel. DIF window has employed for the nodes, which have been interested in the initialization of the frame trade. Time has been also partitioned into the sections in order to hold back from the nodes that have been broadcasted soon after the completion of DIFS. The broadcasting node arbitrarily has selected the section where the broadcast was begun. If any type of accident occurs, then before re-broadcasting sender are required to employ an arbitrary ceased algorithm. In addition, three metrics have been used in order to record the effectiveness and efficiency of IDS, including False negative rate, Detection rate and False positive rate [76-78]. The false negative rate has been developed when the crooked node was labeled as well-mannered [79]. Detection rate has been taking place when the IDS have recognized the crooked node accurately [77, 80]. And the false positive rate has been usually taking place when an IDS has labeled a well-mannered node as an attacker. Some efficient measurements have been launched to improve IDS. Detection latency has been regarded as an essential factor in the measurement of IDS effectiveness and efficiency [81, 82]. In spite of whether the intrusion has been dynamic or static, immediate detection of faults has been helping to respond to them also immediately. The system has been having some disadvantages features such as energy consumption and CPU capacity, which has been known as vital measurements. Time-period for the random nodes has been recorded by Ma et al. [83], so as to drain their efficiency when utilizing an inclined method. The speed of fragmented packets was recorded by Misra et al. [80]. Packet sampling speed has been referring to the packets that IDS has labeled as crooked. The main concept is that no necessity has been proved to consider all the packet bundles when just some of them have prompted IDS. Misra et al.'s architecture has enhanced the fragmented proportion if the detection proportion has been reducing the fragmented proportion, only if the detection proportion has been under the fined threshold.

Table 9: WLAN Attack Type

The speed of Packet sampling must be equal to the detection proportion. The speed of Packet sampling has been associated with the fined threshold whereas detection proportion has been backward linked with the fined threshold. It has been better if the packet sampling speed was high but it could not come at the cost of depressed detection proportion. The difficulty that has been raised here was in the dissection of depressed detection proportion. This has been happening due to the two reasons of depressed ID range or dynamic ID range. The needed time to bring up IDS has been recorded in work by Farid and Rahman [84] and the total time required to thoroughly determine the information content was identified. Also in some research works, researchers have engendered the measurements that visibly do not possess any flaws but do possess some cons. Oppose safety breaches and system capabilities have been recorded by Foo et al. [81]. Shin et al. [85] have amended the decency of nodes mainly in the business field for the deployment of the system. This data has been added in Shin et al. [85] work along with some illegitimate data and even load balances. The concept of how the authors such as Shin et al., Bella et al., and Foo et al., have been used the metrics (reputation, survivability, etc.) in their work have left their argument susceptible. Li et al. have measured performances by using EER from biometric domain [86]. Whether the presented IDS method could have discovered the exact number of intrusions was

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

examined by Haddadi and Sarram [10]. Even though this data has been plain and straightforward but it could not explain everything. Classifications of the relevant metrics for categorization of wireless network attacks have been listed in Table 8. In the consecutive Table 9, various types of network intrusions have been explained by the author. The explanations of wireless and metrics intrusions have been conceiving the matrix of metrics and attacks.

Table 10: WLAN Attack Type (Matrix)

The work has congregated the metrics, which has been classifying a wireless network presented in Table 8 and Table 9. Table 10 has been introducing a matrix that congregates the attack types and the measurements required to classify it. The matrix has been assisting in the collaboration of each intrusion with its metric employed in IDS system.

6. CONCLUSIONS AND FUTURE RESEARCH

Following the objectives of this research, a crystalized concept of intrusion detection was introduced. To do so, three main aspects of intrusion detection known as identification of an unauthorized, illicit, and anomalous behavior were articulated as one might hope. Moreover, the current IDS methodical approaches were classified. So, all classification have been tabulated as well. Ultimately, the WLAN often concepts and the WALN intrusions often interpretations were introduced. So the security vulnerabilities of the WLAN systems were scrutinized along with this different intrusion detection systems in association with WLAN systems were extensively reviewwed. The uniqueness of the research has roots in extracting metrics or features in relation to different attack types. To pinpoint, WLAN has gained high attention throughout, due to the progress that has been made in wireless communication. As the guidelines being set for the computing networks are utilized to observe their security, other intrusion features such as mining can allow the safety measures to be applied to a greater extent. It would have been better if wireless IDS and its efficient and effective measurements have been explored in detail. Detection latency has been mostly used for enhancing the efficiency and effectiveness of IDS. For instance, the IDS would be able to perform better if it adjusts the detection rate based on strength and type of the adversary it faces. Possible repair strategies have been stated to identify the compromised segments and for each one: stop operating, revert all nodes to certified software loads and configurations, rekey/reset passwords and progressively resume operation from the production side of the network towards the consumers. Analysis techniques, which provided early warning of attacks, have been another potential research area. These techniques would be serving as an enabler by providing a promoter for pre-detection responses in WLAN. Another research direction has been distinguishing the early warnings from detections by using confidence level, which accompanies existing analysis techniques.

REFERENCES:

[1] Bhoyar, R., M. Ghonge, and S. Gupta, *Comparative Study on IEEE Standard of Wireless LAN/Wi-Fi 802.11 a/b/g/n.* International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE). (2/7), 2013: p. 687-691.

[2] Taherdoost, H. and A. Keshavarzsaleh. *A Theoretical Review on IT Project Success/Failure Factors and Evaluating the Associated Risks*. in *International Conference on Telecommunications and Informatics. Sliema, Malta*. 2015.

[3] Al-Surmi, I., M. Othman, and B.M. Ali, *Mobility management for IP-based next generation mobile networks: Review, challenge and perspective.* Journal of Network and Computer Applications. (35/1), 2012: p. 295-315.

[4] Pabst, R., et al., *Relay-based deployment concepts for wireless and mobile broadband radio*. IEEE Communications Magazine. (42/9), 2004: p. 80-89.

[5] Wilhoit, K. and S. Hara. *The real world evaluation of cyber-attacks against ICS system*. in *Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference of the*. 2015. IEEE.

[6] Zhong, S., T.M. Khoshgoftaar, and S.V. Nath. *A clustering approach to wireless network intrusion detection*. in *Tools with Artificial Intelligence, 2005. ICTAI 05. 17th IEEE International Conference on*. 2005. IEEE.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Mitchell, R., R. Chen, and M. Eltoweissy. *Signalprint-based intrusion detection in wireless networks*. in *International Workshop on Security in Emerging Wireless Communication and Networking Systems*. 2009. Springer.

[8] Hairui, W. and W. Hua. *Research and design of multi-agent based intrusion detection system on wireless network*. in *Computational Intelligence and Design, 2008. ISCID'08. International Symposium on*. 2008. IEEE.

[9] Sampangi, R.V., S. Dey, and V.N. Viswanath. *The sneeze algorithm: A social network & biomimetic approach for intrusion detection in wireless networks*. in *Business Applications of Social Network Analysis (BASNA), 2010 IEEE International Workshop on*. 2010. IEEE.

[10] Haddadi, F. and M.A. Sarram. *Wireless intrusion detection system using a lightweight agent*. in *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. 2010. IEEE.

[11] Yuan, S., Q.-j. Chen, and P. Li. *Design of a four-layer ids model based on immune danger theory*. in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*. 2009. IEEE.

[12] Eklund, J.M., et al. *Information Technology for Assisted Living at Home: building a wireless infrastructure for assisted living*. in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*. 2006. IEEE.

[13] Gupta, S., S. Kar, and S. Dharmaraja. *BAAP: blackhole attack avoidance protocol for wireless network*. in *Second International Conference on Computer & Communication Technology (ICCCT)*. 2011.

[14] Chen, J., S.-H. Chan, and S.-C. Liew. *Mixed-mode WLAN: the integration of ad hoc mode with wireless LAN infrastructure*. in *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE*. 2003. IEEE.

[15] Sherman, I., *Apparatus for and method of low power wireless local area network independent basic service set mode operation*. 2007, Google Patents.

[16] Karygiannis, T. and L. Owens, *Wireless network security*. NIST special publication. (800/, 2002: p. 48.

[17] Howard, J.D. and T.A. Longstaff, *A common language for computer security incidents*. Sandia National Laboratories, 1998: p.

[18] Ifeagwu, E., M. Alor, and G. Obi, *Received Signal Strength Estimation in Wireless Local Area Network (WLAN) Environment*. 2015: p.

[19] Singh, J., A. Singh, and R. Shree, *An assessment of frequently adopted unsecure patterns in mobile ad hoc network: Requirement and security management perspective*. International Journal of Computer Applications (0975–8887). (24/9), 2011: p.

[20] Lee, I.W. and A.O. Fapojuwo, *Characteristics of wireless LAN traffic*. Proc. WNET. (4/, 2004: p. 674-679.

[21] Sachdeva, S. and R. Malhotra, *A Probabilistic Cell Generation Based Improved Decision Tree Approach for Intrusion Detection*. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org. (3/1), 2015: p.

[22] Singh, R. and T.P. Sharma, *On the IEEE 802.11 i security: a denial-of-service perspective*. Security and Communication Networks. (8/7), 2015: p. 1378-1407.

[23] Kwon, H. and S.-H. Kim, *Efficient mobile device management scheme using security events from wireless intrusion prevention system*, in *Ubiquitous information technologies and applications*. 2013, Springer. p. 815-822.

[24] Noman, H.A., S.M. Abdullah, and H.I. Mohammed, *An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks*. International Journal of Computer Science Issues (IJCSI). (12/4), 2015: p. 107.

[25] Nguyen, T., et al. *An efficient solution for preventing dis' ing attack on 802.11 networks*. 2013. The International Conference on Green Technology and Sustainable Development.

[26] Kumar, R., S. Verma, and G.S. Tomar, *Thwarting address resolution protocol poisoning using man in the middle attack in WLAN*. International Journal of Reliable

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Information and Assurance. (1/1), 2013: p. 8-19.

[27] Shi, Z., et al., *A wormhole attack resistant neighbor discovery scheme with RDMA protocol for 60 GHz directional network.* IEEE Transactions on Emerging Topics in Computing. (1/2), 2013: p. 341-352.

[28] Hu, Y.-C., A. Perrig, and D.B. Johnson, *Wormhole attacks in wireless networks.* IEEE journal on selected areas in communications. (24/2), 2006: p. 370-380.

[29] Pelechrinis, K., M. Iliofotou, and S.V. Krishnamurthy, *Denial of service attacks in wireless networks: The case of jammers.* IEEE Communications Surveys & Tutorials. (13/2), 2011: p. 245-257.

[30] Malekzadeh, M., et al., *Empirical analysis of virtual carrier sense flooding attacks over wireless local area network.* Journal of Computer science. (5/3), 2009: p. 214.

[31] Cam-Winget, N., et al., *Security flaws in 802.11 data link protocols.* Communications of the ACM. (46/5), 2003: p. 35-39.

[32] Rathee, G., P. Bano, and S. Singh, *A study various security attacks in wireless networks.* International Journal of Computer Science and Mobile Computing. (4/, 2015: p. 249-253.

[33] Patil, S. and S. Vanjale, *A Survey on Malicious Access Point Detection Methods for Wireless Local Area Network.* International Journal of Computer Sciences and Engineering. (2/, 2014: p. 22-25.

[34] Khan, S., K.-K. Loo, and Z.U. Din, *Framework for intrusion detection in IEEE 802.11 wireless mesh networks.* Int. Arab J. Inf. Technol. (7/4), 2010: p. 435-440.

[35] Liao, H.-J., et al., *Intrusion detection system: A comprehensive review.* Journal of Network and Computer Applications. (36/1), 2013: p. 16-24.

[36] Ioannis, K., T. Dimitriou, and F.C. Freiling. *Towards intrusion detection in wireless sensor networks*. in *Proc. of the 13th European Wireless Conference*. 2007.

[37] Jadidoleslamy, H., *A hierarchical intrusion detection architecture for wireless sensor networks.* International Journal of Network Security & Its Applications. (3/5), 2011: p. 131.

[38] Abraham, A., et al., *D-SCIDS: Distributed soft computing intrusion detection system.* Journal of Network and Computer Applications. (30/1), 2007: p. 81-98.

[39] Abraham, A., C. Grosan, and C. Martin-Vide, *Evolutionary design of intrusion detection programs.* IJ Network Security. (4/3), 2007: p. 328-339.

[40] da Silva, A.P.R., et al. *Decentralized intrusion detection in wireless sensor networks*. in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. 2005. ACM.

[41] Roman, R., J. Zhou, and J. Lopez. *Applying intrusion detection systems to wireless sensor networks*. in *IEEE Consumer Communications & Networking Conference (CCNC 2006)*. 2006.

[42] Banerjee, S., C. Grosan, and A. Abraham. *IDEAS: intrusion detection based on emotional ants for sensors*. in *Intelligent Systems Design and Applications, 2005. ISDA'05. Proceedings. 5th International Conference on*. 2005. IEEE.

[43] Li, Y. and L.E. Parker. *Intruder detection using a wireless sensor network with an intelligent mobile robot response*. in *Southeastcon, 2008. IEEE*. 2008. IEEE.

[44] Bhuse, V. and A. Gupta, *Anomaly intrusion detection in wireless sensor networks.* Journal of High Speed Networks. (15/1), 2006: p. 33-51.

[45] Alipour, H., et al., *Wireless anomaly detection based on IEEE 802.11 behavior analysis.* IEEE transactions on information forensics and security. (10/10), 2015: p. 2158-2170.

[46] Eik Loo, C., et al., *Intrusion detection for routing attacks in sensor networks.* International Journal of Distributed Sensor Networks. (2/4), 2006: p. 313-332.

[47] Deng, H., Q.-A. Zeng, and D.P. Agrawal. *SVM-based intrusion detection system for wireless ad hoc networks*. in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*. 2003. IEEE.

[48] Huang, Y.-a., et al. *Cross-feature analysis for detecting ad-hoc routing anomalies*. in *Distributed Computing Systems, 2003. Proceedings. 23rd International Conference on*. 2003. IEEE.

[49] Dang, B.H. and W. Li, *Performance evaluation of unsupervised learning techniques for intrusion detection in mobile ad hoc networks*, in *Computer and*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Information Science. 2015, Springer. p. 71-86.

[50] Onat, I. and A. Miri. *An intrusion detection system for wireless sensor networks*. in *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*. 2005. IEEE.

[51] Chen, G., Y. Zhang, and C. Wang, *A wireless multi-step attack pattern recognition method for WLAN.* Expert Systems with Applications. (41/16), 2014: p. 7068-7076.

[52] Mamun, M.S.I. and A. Kabir, *Hierarchical design based intrusion detection system for wireless ad hoc network.* arXiv preprint arXiv:1208.3772, 2012: p.

[53] Sedjelmaci, H. and M. Feham, *Novel hybrid intrusion detection system for clustered wireless sensor network.* arXiv preprint arXiv:1108.2656, 2011: p.

[54] Bhatnagar, R. and U. Shankar, *The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network.* International Journal of Computer Science and Engineering Survey. (3/2), 2012: p. 31.

[55] Yan, K., S. Wang, and C. Liu. *A hybrid intrusion detection system of cluster-based wireless sensor networks*. in *Proceedings of the International MultiConference of Engineers and Computer Scientists*. 2009.

[56] Yan, K., et al. *Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network*. in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. 2010. IEEE.

[57] Hai, T.H., F. Khan, and E.-N. Huh. *Hybrid intrusion detection system for wireless sensor networks*. in *International Conference on Computational Science and Its Applications*. 2007. Springer.

[58] Boubiche, D.E. and A. Bilami, *Cross layer intrusion detection system for wireless sensor network.* International Journal of Network Security & Its Applications. (4/2), 2012: p. 35.

[59] Alrajeh, N.A., S. Khan, and B. Shams, *Intrusion detection systems in wireless sensor networks: a review.* International Journal of Distributed Sensor Networks, 2013: p.

[60] Xiao, M., X. Wang, and G. Yang. *Cross-layer design for the security of wireless sensor networks*. in *Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on*. 2006. IEEE.

[61] Khan, S. and K.-K. Loo, *Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks.* Network Security. (2009/5), 2009: p. 9-16.

[62] Alazab, A., et al., *Developing an Intelligent Intrusion Detection and Prevention System against Web Application Malware*, in *Advances in Security of Information and Communication Networks*. 2013, Springer. p. 177-184.

[63] Shafi, K. and H.A. Abbass, *Evaluation of an adaptive genetic-based signature extraction system for network intrusion detection.* Pattern Analysis and Applications. (16/4), 2013: p. 549-566.

[64] Dilmaghani, R., et al. *Policy-aware service composition in sensor networks*. in *Services Computing (SCC), 2012 IEEE Ninth International Conference on*. 2012. IEEE.

[65] John, S.N., et al. *Creating a Policy Based Network Intrusion Detection System using Java Platform*. in *Proceedings of the International Conference on Security and Management (SAM)*. 2014. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[66] Vigna, G. and R.A. Kemmerer, *NetSTAT: A network-based intrusion detection system.* Journal of computer security. (7/1), 1999: p. 37-71.

[67] Lazarevic, A., V. Kumar, and J. Srivastava, *Intrusion detection: A survey*, in *Managing Cyber Threats*. 2005, Springer. p. 19-78.

[68] Wang, S.-S., et al., *An integrated intrusion detection system for cluster-based wireless sensor networks.* Expert Systems with Applications. (38/12), 2011: p. 15234-15243.

[69] Fragkiadakis, A.G., et al., *Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype.* EURASIP Journal on Wireless Communications and Networking. (2012/1), 2012: p. 73.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[70] Mar, J., et al., *Intelligent intrusion detection and robust null defense for wireless networks.* International Journal of Innovative Computing Information and Control. (8/5), 2012: p. 3341-59.

[71] Modi, C., et al., *A survey of intrusion detection techniques in cloud.* Journal of Network and Computer Applications. (36/1), 2013: p. 42-57.

[72] Sendi, A.S., et al., *Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model.* JNW. (7/2), 2012: p. 311-321.

[73] Li, Y., et al., *An efficient intrusion detection system based on support vector machines and gradually feature removal method.* Expert Systems with Applications. (39/1), 2012: p. 424-430.

[74] Corona, I., G. Giacinto, and F. Roli, *Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues.* Information Sciences. (239/, 2013: p. 201-225.

[75] Bhuyan, M.H., D.K. Bhattacharyya, and J.K. Kalita, *Network anomaly detection: methods, systems and tools.* Ieee communications surveys & tutorials. (16/1), 2014: p. 303-336.

[76] Tao, Z. and A. Ruighaver. *Wireless Intrusion Detection: Not as easy as traditional network intrusion detection*. in *TENCON 2005 2005 IEEE Region 10*. 2005. IEEE.

[77] Xiao, Z., C. Liu, and C. Chen. *An anomaly detection scheme based on machine learning for wsn*. in *Information Science and Engineering (ICISE), 2009 1st International Conference on*. 2009. IEEE.

[78] Han, H., X.-L. Lu, and L.-Y. Ren. *Using data mining to discover signatures in network-based intrusion detection*. in *Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on*. 2002. IEEE.

[79] Svecs, I., et al. *Xidr: A dynamic framework utilizing cross-layer intrusion detection for effective response deployment*. in *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*. 2010. IEEE.

[80] Misra, S., P.V. Krishna, and K.I. Abraham. *Energy efficient learning solution for intrusion detection in wireless sensor networks*. in *Communication Systems and Networks (COMSNETS), 2010 Second International Conference on*. 2010. IEEE.

[81] Foo, B., et al. *ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment*. in *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*. 2005. IEEE.

[82] Ko, C., M. Ruschitzka, and K. Levitt. *Execution monitoring of security-critical programs in distributed systems: A specification-based approach*. in *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*. 1997. IEEE.

[83] Ma, Y., H. Cao, and J. Ma. *The intrusion detection method based on game theory in wireless sensor network*. in *Ubi-Media Computing, 2008 First IEEE International Conference on*. 2008. IEEE.

[84] Farid, D.M. and M.Z. Rahman. *Learning intrusion detection based on adaptive bayesian algorithm*. in *Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on*. 2008. IEEE.

[85] Shin, J., T. Kim, and S. Tak. *A reputation management scheme improving the trustworthiness of p2p networks*. in *Convergence and Hybrid Information Technology, 2008. ICHIT'08. International Conference on*. 2008. IEEE.

[86] Li, F., et al. *Behaviour profiling on mobile devices*. in *Emerging Security Technologies (EST), 2010 International Conference on*. 2010. IEEE.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

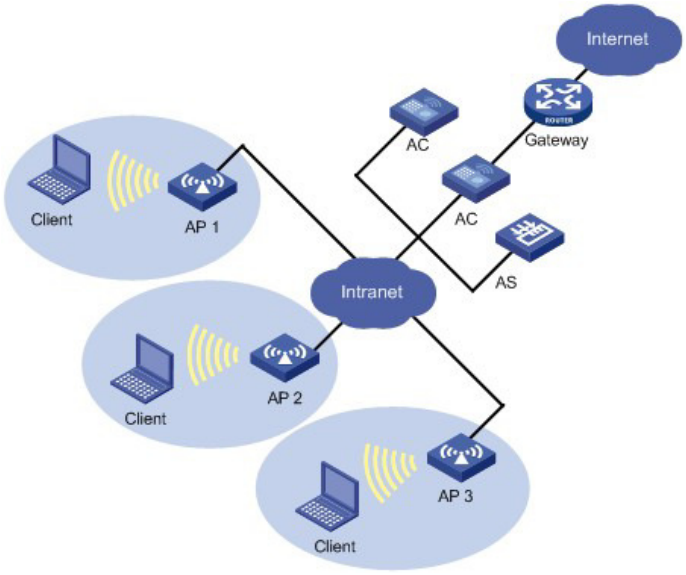

Figure 1: WLAN Basic Model

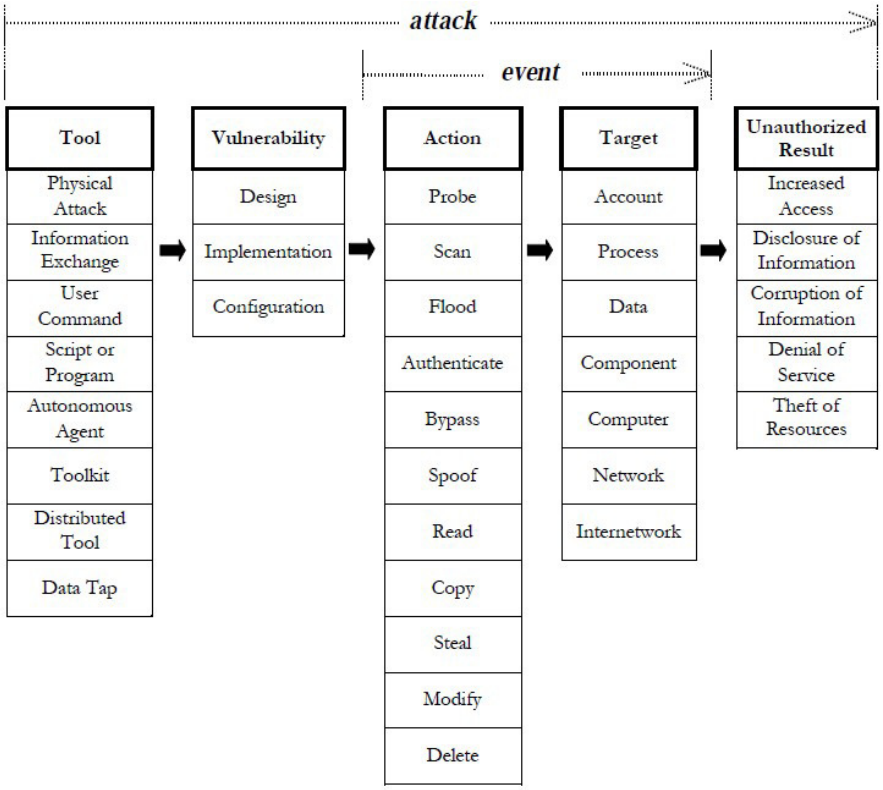

Figure 3: Howard's Taxonomy of Attacks

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

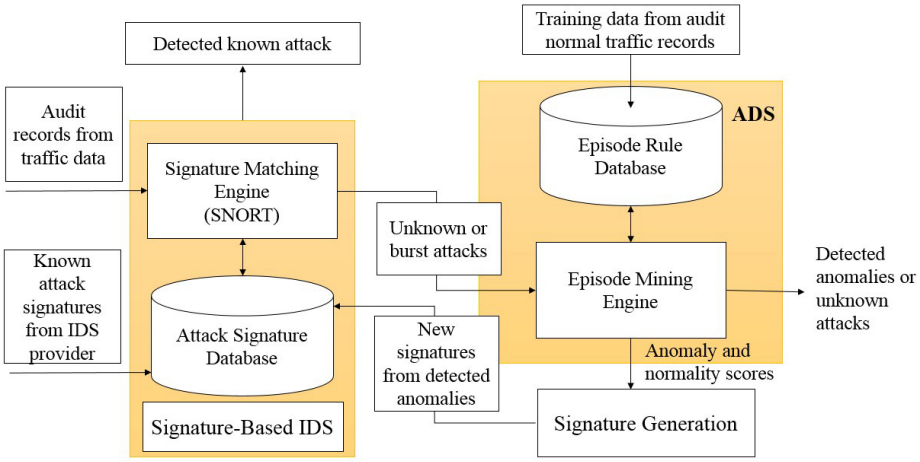

Figure 4: Hybrid IDS

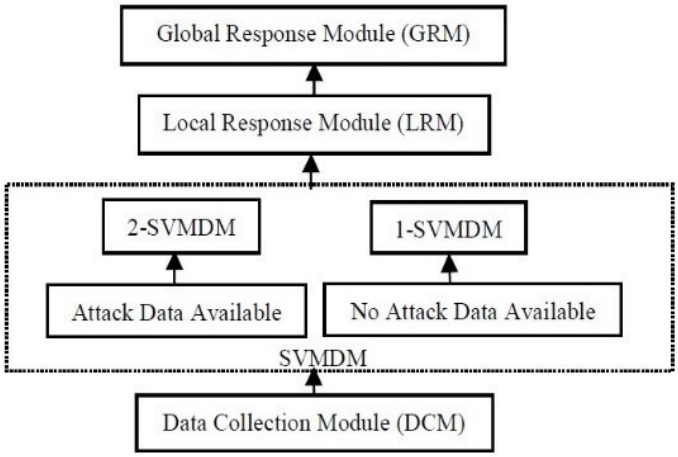

Figure 5: Cluster-based Hybrid IDS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Signature-based Technique and Associated IDSs.

Mechanism	Attacks	Evaluation metrics	Ref.
Collaborative	Black hole, selective forwarding	Window length, false negative rates	[30]
Local and cooperative detection	Sink hole	Detection rate, false negative rates	[31]
Hierarchical	N/A	N/A	[32]
Genetic programming	DoS, unauthorized access	Classification accuracy	[33]
Soft computing	Unauthorized access, probing	Classification accuracy	[34]
Specification based	Repetition attack, delay attack, worm hole, alteration attack, black hole, selective forwarding	Detection rate, false positives	[35]
Spontaneous watchdog	N/A	N/A	[36]
Ant colony	Abnormal transmission	N/A	[37]

Table 2: Anomaly based Technique and Associated IDSs.

Mechanism	Attacks	Ref.
Artificial neural network	Time related changes	[38]
Set of techniques at OSI layers	Masquerade, routing Attacks	[39, 40]
Cluster based	Periodic route error attack, sink hole attack	[41]
Support vector	Black-hole attacks	[42]
Cross feature	Packet dropping attacks	[43, 44]
Sliding window	Route depletion attack	[45]

Table 3: Hybrid Technique and Associated IDSs.

Mechanism	Attacks	Ref.
Hybrid, hierarchical	N/A	[47]
Support vector machine	N/A	[48]
State transition	Sync flood	[49]
Cluster based	Routing attacks	[50]
Cluster based, supervised learning, misuse	Routing attacks	[51]
Hierarchical and hybrid	Sink hole, worm hole	[52]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: A Comparison among IDSs.

Characteristics	Signature based IDS	Anomaly based IDS	Hybrid IDS	Cross layer IDS
Detection rate	Medium	Medium	High	High
Attack detection	Few	Few	More	More
Computation	Low	Low	Medium	High
False alarm	Medium	Medium	Low	Low
Energy consumption	Low	Low	Medium	High
Multilayer attack detections	No	No	No	Yes
Weakness	Cannot detect new attacks	Misses well known attack	Requires more computation and resources	Requires more resources
Strength	Detects all those attacks having signatures	Capable of detecting new attacks	Can detect both existing and new attacks	Can detect multilayer
Suitable for WLAN	Yes	Yes	Yes	Yes with modification

Table 5: Advantages of IDS for WLAN and Ad-hoc Networks.

	WLANs	Ad hoc networks
Signature based	Variable CONOP, Easy updates	High detection rate
Anomaly based	Unknown attacks	Unknown attacks
Reputation based	Find selfish actors	Find selfish actors
Specification based	Unknown attacks	Unknown attacks
Traffic based	Metadata rich	Metadata rich
Multi-trust	Expanded data set	Expanded data set
Behavior based	Low false negatives	Minimal memory

Table 6: Disadvantages of IDS for WLAN and Ad-hoc Networks

	WLANs	Ad hoc networks
Signature based	Dictionary freshness	Dictionary freshness
Anomaly based	Variable CONOP, High false positive	Variable CONOP, High false positive
Reputation based	Selfish actor sanctions	Selfish actor sanctions
Specification based	Lack common use cases	Lack common use cases
Traffic based	Inconsistent visibility	Inconsistent visibility
Multi-trust	Dynamic population	Dynamic population
Behavior based	Erratic profiles	Erratic profiles

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7: Intrusion Detection System Classification in WLAN.

Detection approach		Methodology			Technology Type	Time series	Attacks Detection	Performance	Ref.
		AD	SD	SP					
Pattern-based	Pattern Matching	×	×	×	N	×	K	H	[62, 63]
	Perti Net	×	×	×	H	×	K	M	
	Keystroke monitoring	×	×	×	H	×	K	H	
	File system checking	×	×	×	H	×	B	H	
Rule-based	Rule based	×	×	×	H/N	×	B	H	[64, 65]
	Data Mining	×	×	×	N	×	B	M	
	Model/Profile-based	×	×	×	H/N	×	U	M	
	Support vector machine (SVM)	×	×	×	N	×	B	H	
Statistics-based	Statistics	×	×	×	H/N	×	B	M	[65, 66]
	Distance-based	×	×	×	N	×	U	M	
	Bayesian-based	×	×	×	N	×	B	H	
	Game Theory	×	×	×	H/N	×	U	L	
Heuristic-based	Neural Networks	×	×	×	N	×	B	M	[64, 66, 67]
	Fuzzy Logic	×	×	×	H/N	×	U	H	
	Genetic algorithm	×	×	×	N	×	K	L	
	Immune system	×	×	×	H	×	B	M	
	Swarm Intelligent (SI)	×	×	×	N	×	U	H	
State-based	State-Transition Analysis	×	×	×	H/N	×	K	H	[68, 69]
	User intention Identification	×	×	×	H	×	U	H	
	Markov Process Model	×	×	×	H/N	×	U	M	
	Protocol Analysis	×	×	×	P	×	T	L	

Table 8: Classification of Relevant Metrics for WLAN Attacks

Metric code	Metric Name	Metric code	Metric Name
M1	MAC Address	M19	ARP ⁄ IP pair change
M2	OUI	M20	Static / Dynamic IP
M3	Broadcast SSID	M21	SSL/Encryption in use / WEP
M4	IP address	M22	Antenna type
M5	Change of MAC allowed in NIC	M23	VPN in use
M6	Sequence number of Client	M24	Retry bit in control frame
M7	Sequence number of AP	M25	Spoofed disassociate msg
M8	2-bit state (Unauth & Associated)	M26	802.1 x extensions in use
M9	Class 1 frames RTS/CTS/ACK/POLL	M27	Buffer overflows allowed
M10	NIC Vendor	M28	PPP enabled
M11	Deauth msg +spoofed msg	M29	Ad-hoc Network
M12	Reason code	M30	Authentication attempts
M13	Packer leash	M31	Loops / alternate routes
M14	Timeout for RTS	M32	3DES orRC4
M15	Frad headers	M33	MAC list in AP
M16	NIC in promiscuous mode	M34	CCM Mode
M17	Switch ⁄ hub	M35	TKIP
M18	MAC address overload	M36	Signal Noise ratio

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 9: WLAN Attack Type

Metric code	Metric Name	Metric code	Metric Name
A	MAC Address Spoofing	A	Packet Alteration
A	Bypassing Access control lists	A	Packet Re-routing
A	Authenticated user impersonation	A	Packet Insertion
A	Invalid State	A	Denial of Service
A	Reauthentication	A	War Driving
A	Disassociation	A	Main-in-the-Middle Attack
A	RTS/CTS Flood	A	High Power amplifiers
A	Fragmentation Attacks	A	Multiple virtual Access points
A	ARP Poisoning	A	MAC Based inference of ACL
A	Work hole Attacks	A	Dictionary Attack - WPA
A	Network Injection Attacks	A	Virtual carrier sense attack

Table 10: WLAN Attack Type (Matrix)

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
M1	×	×									×									×		
M2	×																					
M3											×				×					×		
M4													×		×							
M5	×	×																		×		
M6	×																					
M7	×																		×			
M8					×																	
M9							×															×
M10	×																			×		
M11					×																	
M12						×																
M13										×		×	×	×								
M14							×															
M15								×														
M16									×													
M17									×													
M18									×													
M19									×													
M20									×													
M21									×						×		×				×	
M22										×					×	×		×				
M23											×						×	×				
M24																×						
M25				×		×																
M26		×	×					×				×	×	×		×			×			×
M27						×																
M28																	×					
M29						×										×						
M30	×			×																	×	
M31											×											
M32			×																			
M33		×																				
M34								×														
M35								×														
M36																		×				