EEWIPS: An Enactment Evaluation of Wireless Intrusion Prevention System for Wireless LAN

S V Athawale[1], Dr M A Pund[2]
[1]Dept of Computer Engineering
[2]Dept of Computer Science & Engineering
[1]SGBA,Amravati University,Amravati,India
[2]PRMIT & R, Badnera – Amravati.

Abstract*- This paper instants an Enactment Evaluation of wireless LAN that may accustom the value of performance and effectiveness of wireless intrusion prevention system. Recently, involuntary computing methods are widely used for intrusion prevention system. Intrusion Prevention Systems- it's the Next Step in the Evolution of IDS although some [1] wireless intrusion prevention systems (WIPS) exist in the market, recent studies show that wireless networks are still liable to advanced, dynamic, and knowledgeable attacks. During this paper, we review current wireless intrusion prevention systems and evaluate their performance to sight a large vary of wireless network attacks. To judge the performance of WIPS, we have a tendency to use many performance metrics to quantify the accuracy, extendibility, ability, measurability, overhead, and latency of the examined WIPS. Our experimental results show that this Enactment Evaluation will reveal different weaknesses within the examined WIPS.*

Keywords- Enactment Evaluation, LAN, IDS, WIPS, Wireless Network Security.

I. INTRODUCTION

Wireless native space Networks (WLAN) square measure taking a increasingly crucial role in fashionable society; but, the dearth of effective and cheap security measures created them simple targets for intruders, Particularly once operational in unsecured open mediums. Demonstrates [2] that almost all established wireless security tools square measure deployed simply toward large-scale enterprise networks and neglect smaller networks; states that larger companies still have considerations that forestall them from wide utilizing WLAN. To find or forestall wireless attacks, some security ways are projected. Wireless Intrusion Detection Systems (WIPS) is generally classified into 2 types: anomaly-based detection and signature-based detection systems. Lee associated [3] state that the performance of an Intrusion Detection System (IDS) is evaluated in step with the subsequent 3 procedures: accuracy, extendibility, and adaptableness. Accuracy is measured by the false positive and negative rates; extendibility measures the flexibility for change a WIPS; and adaptableness is thought-about by the time and price for change a WIPS. During a previous analysis, we have a tendency to bestowed anomaly-based intrusion detection system (WIPS) that's supported multi-channel on-line observation and anomaly analysis of station localization, frame behavior, and network access violations with relevancy multiple-observation time windows. WIPS monitors wireless networks, generates network options, tracks Wi-Fi access state machine violations, generates wireless network flows for multiple time windows, and uses the dynamically updated anomaly and misuse rules to find complicated known and unknown wireless attacks and take acceptable proactive actions.

The rest of this paper is organized as follows: Section two surveys the Wi-Fi attacks, and reviews this intrusion detection ways. In section three, we have a tendency to transient WIPS methodology. Section four presents the analysis methodology. Section five presents the analysis work and experimental results. Section six presents the outline and closing results.

II. RELATED REASERCH WORK

A. Categorize of Wireless Network Attacks

Wireless attacks exploit and manipulate computing and/or wireless network resources. They're capable of degrading the wireless network performance and shatter users' privacy. During this section, we have a tendency to gift a survey of wireless attacks, and compensatory approaches. Wireless network attacks are often classified into six categories: Identity spoofing, Eavesdropping, Vulnerability, Denial of Service (DOS), Replay, and scallywag Access purpose attacks. In supply MAC and science address spoofing, attackers will hide their identities by victimization totally different MAC and/or science addresses from those wrongfully allotted to them.

There are three differing types of MAC spoofing attack: random, vendor-oriented, and peer [16]. Random MAC spoofing is to every which way generate a MAC address; vendor- familiarized is semi-random wherever attackers will generate a random MAC address however opts for the primary 1/2 the address, that represents the seller code; and peer spoofing is to repeat a MAC address of 1 of the users within the network. Eavesdropping attacks are often classified into traffic analysis, and passive or active eavesdropping. A traffic-analysis attack happens once the offender uses a high gain antenna to get data like signal power, supply sort, and packet size; attackers during this class might or might not interfere with communication channels [4]. Passive eavesdropping transpires once attackers sniff users' packets while not officious with the communication channels; attackers will collect data like the packet digest to be decrypted and analyzed. Active eavesdropping happens once attackers inject probe request frames into a communication medium to uncover silent access points and user stations. Vulnerability attacks profit of wireless network protocol style errors; greedy behavior will comprise this class [5] .The fourth wireless attack class is Denial of Service attacks like beacon, probe request, association, authentication, ARP, and information flood attacks; attackers will flood the network with useless traffic and slow or maybe block legitimate users from accessing wireless network resources ; samples of this attack embrace authentication frame attack, that de-authenticates shoppers from a particular AP; filling up AP association and authentication buffers; physical layer attacks; disassociation frames floods; and network setting attack, like management frame attacks. Some wireless DOS attacks target the 802.11i implementation like EAP authentication attacks. additionally, wireless networks are susceptible to wired-inherited Denial of Service DOS attacks like TCP-SYN attack, Smurf science attack, and ICMP flood attack they will break through the attacked local area network to severely degrade service performance and eventually pack up the whole network; [6] sleuthing these attacks early at their wireless sources can save networks important harm and destruction.

Replay attacks occur once offenders record wireless network traffic and replay them at totally different times; these attacks enable the attacker to access network resources while not victimization access keys. Scallywag Access Points like Wireless Repeater, Access Points connected to secure wired network, Honey-pot, and Man-In-The-Middle (MITM) that allows attackers to insert themselves between the users and therefore the real AP, that permits them to scan and modify the info contents. Session High-jacking happens once attackers will take over a session from a legitimate user and create the user assume that it's an awry within the wireless network; official. [7] Describe a lot of wireless attacks during this class like Address Resolution Protocol (ARP) poisoning attack, and de- authentication attack that convinces users that the AP is asking them to reset their connections.

B. Current Wireless Security Techniques

Current wireless network defense tools believe totally on pre-defined attack signatures for detection. Whereas those ways will with success discover normally best-known attacks, they can't acknowledge abnormal behavior caused by new and complex attacks till it's doubtless too late to require any helpful action within a wireless network; those tools may additionally fail to discover kinds of acknowledge attacks that area unit launched in an exceedingly non-traditional approach mentioned in section a pair of.1. The intrusion-detection systems that use anomaly analysis don't seem to be wide used and effective thanks to the high false alarms they generate. Ref. [8] instructed that any new approach should address the wireless security supported the wireless medium characteristics. Wireless security system is classified into 2 types: intrusion detection, or intrusion detection with response. Wireless Intrusion Detection Systems' (WIDSs) goal is to discover early signs of wireless attacks therefore correct response is implemented. WIDSs collect wireless activity knowledge and analyze the knowledge to uncover attacks with minimal false positive and negative rates. Anomaly based mostly systems [9] discover wireless attacks in line with reference models of traditional behavior. Ref. [10] presents Associate in Nursing anomaly-based approach to discover makes an attempt to utilize further information measure in IEEE 802.11 hotspots; it collects applied math knowledge concerning network's traditional behavior, and set anomaly thresholds to discover makes an attempt for utilizing further information measure of channels; the attributes utilized in [11] area unit output and back-off. Ref. [11] uses anomaly-based methodology to discover the variation of device location from antecedently learned location data. Misuse-based wireless intrusion detection ways generate alerts supported well-known attacks or system weaknesses to spot best-known intrusions. Ref. [1] presents a misuse-based approach to get alarms of man-in-the-middle attack victimization sequence variety violations and de-authentication frames; though this approach counts the quantity of attack de-authentication frames, it's still thought-about misuse as a result of it uses attacks thresholds. Specification-based wireless intrusion detection ways use a collection of rules or policies that outline the proper operation of a protocol, and compare the behavior with relevancy outlined policies. Ref. [3] presents Associate in nursing approach supported rules derived from the network state transition models; it profiles the conventional activity of the network traffic with relevancy the network state machine policies and detects any discrepancy from those policies. There is unit completely different WIPS industrial merchandise accessible on the market. Suricata utilizes a collection of sensors connected to a centralized server that may be interfaced with a secured web; Suricata differentiates between attacks and security events, and is principally involved in police investigation scallywag access points; it addresses the difficulty of Macintosh address spoofing by chase the network card characteristics forward that the user and therefore the assaulter use completely different wireless network cards; though there's an honest likelihood that the idea might not hold, this tool will facilitate in police investigation some intruders [10]; Suricata can force Associate in Nursing interloper to part from a legitimate network. Air magnet detects scallywag access points and DOS flooding attacks and doesn't need hardware implementations; Air magnet will discover IEEE 802.11 b/g overlapping channels. Airsnare will discover unauthorized Macintosh addresses to attach to an AP. Wisentry differentiates between trustworthy and untrusted devices and provides a configurable alert info. AWIPS [1] is anomaly-based and might accurately discover a good vary of wireless network attacks. Unlike alternative WIDSs that area unit signature-based, AWIDS will discover slow and fast DOS attacks or attacks that don't seem to be learned by the system. AWIDS generates responses like generating different alerts, locating and de-authenticating attackers, change access management list, and change detection rules to safeguard the legitimate users' privacy, and save the network from to any extent further injury.

III. WIPS INTRODUCTION

In a previous analysis, we tend to planned associate degree Anomaly-Based Wireless Intrusion Detection System (AWIDS) [1]. AWIDS approach relies on multi-channel on-line watching, and anomaly analysis of station localization, frame behavior and network access violations with regard to multiple-observation time windows. AWIDS has the subsequent features: it monitors wireless networks, generates network options, tracks wireless-network-state machine violations, generates wireless network flows (WNetFlows) for multiple time windows, and uses the dynamically updated anomaly and misuse rules to discover complicated acknowledged and unknown wireless attacks and take acceptable proactive actions. the target of AWIDS mechanism is to discover complicated wireless attacks and generate counter measures to shield the local area network and also the privacy of the users. It uses a group of activity attributes collected from multiple wireless channels that has info from signal analyzer, and packet monitor. Wireless Network Flows (WNetFlows) square measure learned and deep-mined to pick out the options that square measure most relevant to differing types of traditional traffic and attacks. AWIDS anomaly behaviour analysis engine uses each customary and coaching based mostly anomaly behavior analysis; and sends alerts to a prediction engine that determines the attack kind, and sends completely different info regarding the attack and also the assailant to the impact analysis module that determines the suitable action supported risk analysis and pass that to the action handler to require the suitable response. almost like NetFlow [17], Wireless-Network Flow (WNetFlow) provides necessary info regarding wireless network users and applications. Owing to specifications in wireless networks, Fayssal and Hariri [1] introduced completely different structure for WNetFlow than the NetFlow employed in wired network. WNetFlow provides info regarding applications, wireless-network channel usage, wireless signal illation, wireless network anomaly and security vulnerabilities, still because the impact of changes and anomalies on the wireless network performance.

WNetFlow square measure used for Wireless network anomaly behavior analysis; WNetFlows square measure made and fed to a classifier to come up with rules; that square measure accustomed discover complicated wireless attacks and utilized by the action module to require the suitable response. Every WNetFlow consists of a WNetFlow-key and alternative supplementary options. WNetFlow secret is composed of a group of great options collective into one key; those options square measure the common attributes between all WNetFlows elect to discover a selected traffic kind. The knowledge provided by the WNetFlow secret is later utilized by the action module.

IV. ASSESMENT METHOD

Traditionally, the performance is measured by the false positive and negative rates; though those metrics area unit essential, different metrics like extendibility, ability, scalability, overhead, and latency will be necessary and may be thought-about. We have a tendency to propose a holistic analysis approach that considers the on top of metrics. Those metrics are accustomed measure the performance of WIDSs throughout normal traffic and for various kinds of attacks

A. Network Accuracy

Accuracy of associate degree IDS is measured by its false-positive alerts and intrusion detection rate (DR). A false positive (FP) means that associate degree IDS generates associate degree alert accusatory sure network traffic or resource of behaving abnormally, when that is not the case. To use a typical methodology for calculating the false-positive rate between totally different research and business systems, we have a tendency to verify FPR from both traditional traffic and also the background normal traffic during the attack, and is measured by the share of normal connections classified as intrusions as given in Equation 1a and 1b:

$$False\_Positive = \sum_{t=1}^{t=T} FP(\mathrm{t})$$

$$(1)\ FPR = FP / \mathrm{total\_normal\_frames} \qquad (2)$$

False Negative Detection (FND) arises once no alert appears within the case of intrusion. The detection prevention rate (DPR) is computed because the proportion of times a precise attack kind is detected once the attack is launched n times every in different attack variation as given in Equation 2:

$$DPR_k = \sum_{l=1}^{n} N_{l,\,k} / \mathrm{n}, \mathrm{N} = \{\mathrm{T}, \mathrm{F}\}$$

Where n is the total number of variations for attack type l;k is T if the attack is detected and F if the attack is not detected.

B. Extendibility and Adaptability

Extendibility is that the ability of a system to adapt to new environments, whereas ability is that the dynamic configuration support of a system to adapt to those changes. Adaptation issue (AF) is outlined because the adaptability quantitative mensuration. AF will enclose each extensibility and adaptableness considering a system that's not protractile (rigid) as having high AF. Ability Degree (AD) provides another variety of ability quantification victimization the AF with system specifications from experimental analysis. To quantify the extendibility and adaptableness (i.e., development effort) of a system, we have a tendency to use perform purpose analysis (FPA) target-hunting by its 5 major parts which will be classified into information functions and transactional functions. information functions square measure evaluated by internal logical files (ILF) and external interface files (EIF); ILF allows the user to take care of the Logical groupings of information in an exceedingly system (e.g., process the detection thresholds before running the system); EIF refers the user to use information from external systems for referencing (e.g., victimization another intrusion detection system to verify the generated alerts of the tested system or use another localization tool that views the network from a special geographical area). Transactional functions embody external input (EI), external output (EO), and external enquiries (EQ); EI provides the power for a user to feature, delete and alter the info (e.g., the user will add, delete, and update detection rules before or throughout the run time); EO provides the user the power to supply the output (e.g., users will filter the displayed alerts per the channel, STA, and/or AP); combining weight allows the user to store information so retrieve it (e.g., store the log information, packet information into files and be able to retrieve it on demand). we have a tendency to developed a trial quantification methodology with 3 levels of quality , high suggests that the system isn't long, low implies that the system is already adaptive, and average implies that the system is long however not nevertheless machine-controlled. The overall AF is calculated as given in Equation three.

$$AF = \sum_{i=1}^{n} C_i \qquad (3)$$

For every n purposeful points with quality C ability Degree (AD) ∈ [T,F] is that the quantitative mensuration of ability between T, and F means the system altogether variable and F means the system isn't extendible as given in Equation three.

C. Scalability, Latency and Overhead

Scalability could be a crucial issue for performance analysis of WIDSs. It quantifies the WIDS ability to handle a bigger range of APs and STAs situated within the watching space. The overhead is outlined because the quantity of resource consumption. We have a tendency to use processor overhead as a measure tool. quantifiability and overhead area unit interconnected as a result of a ascendable system mustn't crash beneath significant traffic or larger range of nodes. If a system will handle larger range nodes however not traffic, it cannot be reliable. Latency for Dynamic Configuration outlined because the time required in coming the system to traditional state once the invention of false actions. Throughout runtime, interval of actions to discovered attacks measures the sensitivity of the system to setting changes. Slow response isn't essentially unhealthy, as a result of it saves the system configuration of being often modified.

This metric isn't employed in the experimental analysis as a result of each experimented systems don't implement dynamic configuration

V. EXPERIMENTAL EVALUATION

The analysis method includes totally different parts such as making ready and managing the work, managing the background traffic, testing the evaluated systems, launching attacks, re-testing constant systems, and analyzing the evaluated WIDSs results. The higher than method includes mechanically labeling attacks (i.e., tagging each packet related to every launched attack); though this method is machine-driven, it needs plenty of manual revisions owing to the specification of every attack, where some attacks area unit labeled by supply waterproof address, others by destination waterproof address, whereas some area unit labeled by channel. Post evaluation analysis is important to look at the reason a system misses a particular attack and what improvements may be done to sight it. The work shown in Figure-1 consists of access points (APs) and includes totally different encoding strategies in every experiment.

The test-bed uses eight machines acting as wireless stations (STA) generating traditional traffic from a ready normal traffic library. The work conjointly includes some wired machines connected to constant switch that connects the tested wireless access points. The AWIPS multi-channel observance station may be a UNIX operating system (fedora-20) machine equipped with high gain antennas capable of monitoring an oversized geographic area on all the 802.11b wireless channels in use [1 through eleven while not channel hoping] additionally to the wired LAN that's utilized by the wireless access points. Suricata Mobile and private is implemented on a robust Windows XP laptop computer machine configured with Linksys-WPC55AG wireless network card. Also, we have a tendency to organized Associate in nursing offender machine that targets the users of the attacked access purpose. In our work, we used the Windows 7, Windows visual percept and UNIX operating system operating systems for the STA machines.

We created traffic manager that generates end-to-end traffic flows that imitate applications and/or users' behaviors. The acceptable traffic kind satisfies totally different constraints like packet size, payload content, traffic frequency, choice of network services, and other behavioral characteristics. The traffic library includes application level traffic, HTTP, FTP, Video streaming, Voice-over-IP, additionally to layer two traffic that features normal beacon, probe and association requests. Also, the library is programmed to attach to the secured and unsecured wireless networks exploitation predefined WEP and WPA keys. Our tools area unit capable of launching many attacks like waterproof and IP spoofing, waterproof address generation, passive eavesdropping, active eavesdropping, spoofed de-authentication, authentication frame flood, WEP cracking, WPA cracking (with weak password), association packets, ARP floods, probe request slow/fast flood, beacon slow/fast flood, traffic analysis, rogue access points, replay attacks, spoofed disassociation, MITM, and plenty of others. Additionally, we have a tendency to use some attack tools transmissible from the wired network attacks like TCP SYN, ICMP and UDP floods. The later attacks will go beyond the wireless network; they aim totally different services on the web.

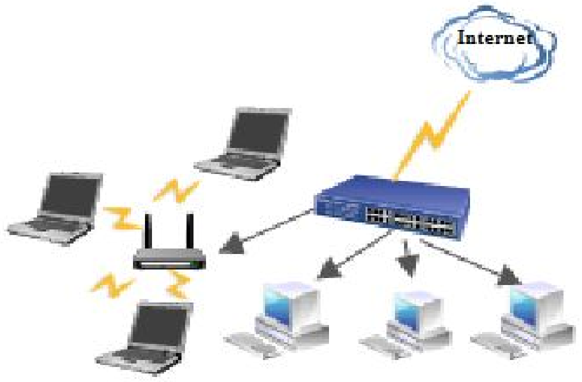

Fig. 1. Experimental scenario with adaptability and scalability and Accuracy, Latency and system overhead

A. System Adaptability and Scalability

We compare the ability of AWIPS approach and also the Suricata consistent with twenty seven perform points and also the complexity is equally weighted giving 3 levels of development complexness High =2 (not extendable), Average = one (system long however issue not implemented), Low = zero (implemented), if the system is totally rigid, this ends up to maximum rate AF = 55 given N = 1 leads to AD = 0.0057 that's near 1/3. A totally adaptive system (fully automated) has AF = zero ends up in AD = one or 100%. Table 1 shows the AF and AD for each AWIDS and Suricata.

Table 1.Adapability of AWIPS

	AWIPS	Suricata
Functional Points Evolution	25 Functional Points	25 Functional Points
AF	7	19
AD	57.24%	19.67%

The measurability is measured by the overall range of APs and STAs that a system will handle. AWIPS doesn't have any limitation there on; it will handle any network size but might suffer higher system overhead for larger networks. Suricata, doesn't state any limitations on the maximum range of APs and STAs and our experiments show that it's ascendible to suit giant networks of tens of APs and STAs

B. Accuracy, Latency and system Overhead

System behavior throughout the conventional network operation might dramatically amendment at the time of attack particularly within the case of intensive attacks. We tend to use those metrics to judge [12], [13] those systems throughout mistreatment traditional traffic and twenty two forms of attack. To generate traditional traffic, we tend to develop a traffic generator that imitates the conventional wireless network user traffic. We tend to injected around 508537 packets of traditional traffic in ten separate runs throughout a 10-hours amount. Conventional traffic enclosed normal user affiliation and disconnection to check the conventional operation of wireless users.

The overhead of the tested systems is measured by the electronic equipment consumption. For traditional traffic operation AWIPS electronic equipment consumption exaggerated from a mean of 4.74% to an average of 17%; whereas AWIPS exaggerated the electronic equipment consumption from a mean 4.76% to 16.5%. Figure two shows the false positive rate for ten totally different sets of traditional traffic collected at separate times. AWIDS committed a complete range false alert of 449 compared to 1760 for Suricata, wherever the full range of records altogether traditional datasets is 518539, Figure 2 shows the precise range of false alerts in every dataset for each AWIPS and Suricata. De-authentication Attack to check the performance of the examined WIPS, we tend to launched de-authentication attack with ten totally different attack variations. The de-authentication attacks are often launched in 3 modes: from a spoofed AP to any or all the users, to selected users, or broadcast; for every [14] mode, the attack will have totally different intensities starting from one to 2500 frames per second. To disconnect a user station and demonstrate it to a different AP, it needs a minimum of one frame; our experiments show that eight de-authentication frames were enough to disconnect all users altogether the experiments. In every our experiments, we tend to collected the quantity of false alerts and noted the detection standing. De-authentication attacks are often terribly slow or in no time. In case of slow attack, the typical electronic equipment overhead is sort of identical as traditional traffic. In no time de-authentication attacks the electronic equipment consumption will increase to a median twenty seventh, [15] whereas AWIPS will increase the typical electronic equipment consumption to twenty ninth. Suricata doesn't sight this attack if it targets the users directly; it solely works within the case of broadcast. Within the case of AP-> Broadcast, Suricata detected the attack if the intensity is above 22 frames resulting in a mean detection rate of 29.57%. AWIPS will sight all the modes and variations of this attack.

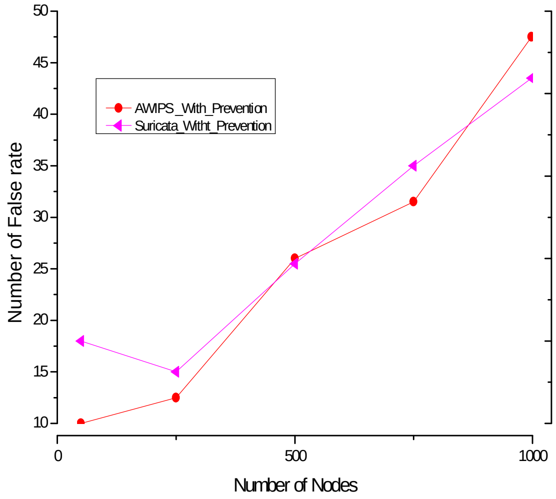

Fig. 2. Number of False rate with Normal traffic nodes.

Wireless Scanning Attack

Scanning attack is that the first stage of organized wireless attacks. Scanning attacks will passive or active, passive attacks don't seem to be attainable to be detected, whereas active attacks are often half-tracked tho' signatures or activity. We tend to launch this attack mistreatment Commview Wi-Fi in several modes; in some cases, we tend to scanned all channels and in different cases we tend to restrict our scan to some channels. Also, we used traffic analysis tools like Netstumbler. This attack could also be not intensive however might cause the intrusion detection to make giant overhead on the system as a result of it forces the STAs and APs to reply to the scanning requests. Suricata C.P.U. consumption inflated traditional to a median of 23%, whereas AWIPS increase to a median of 20.7%.Both Suricata and AWIPS were able to discover this attack.

Flood Attack with Reassociation

This attack is often dangerous as a result of it targets the primary state of the 802.11/802.11i state machine, wherever it can't be detected by standard-based WIPS. We tend to launch this attack in 9 totally different intensities locomotive between 12 and 2500 frames per second.

The overhead during this attack comes from the massive quantity of sniffed frames to be processed. AWIDS functions on all eleven channels thus it will add a lot of overhead of twenty three.15% throughout this sort of attacks. Suricata uses channel hopping that needs less process and ends up in overhead of twenty-two.27%.

Suricata detected this attack classified it as non essential event (association event). If we tend to think about the event alerts as attack alerts, the typical detection rate of Suricata is 87.69%; AWIDS detected all variations of this attack.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have a tendency to given a framework to guage the performance of wireless intrusion detection systems (WIPS). The projected framework relies on a brand new classification model for wireless attacks; and a collection of metrics that live the performance of WIDSs. Those metrics quantify the overhead, quantifiability, ability, extendibility, accuracy, and latency of the examined systems. We have a tendency to applied this technique to check the performance of 2 systems: Anomaly-based wireless intrusion detection system (WIPS), and Suricata. Our results show that WIPS is a lot of correct with a detection rate of 99.16% compared to 43.4% for Suricata; additionally, WIPS is a lot of adjustable with ability degree of 57.45% compared to 19.79% for Suricata; however Suricata creates less overhead on the system of a median of 20.33% compared to 20.45% for WIPS. We have a tendency to area unit presently researching on rising WIPS automatic response system to self-discover and proper false positives; this improvement will cause having an entire anomaly-based wireless self-defense system.

VII. ACKNOWLEDGMENT

The authors would really like to give thanks the anonymous reviewers for valuable comments to improve the standard of the paper.

REFERENCES

[1] Samer Fayssal, Byoung Uk Kim, Performance analysis Toolset for wireless intrusion detection systems , High Performance Computing and Simulation (HPCS), 2010 International Conference,2010.

[2] R. Dorus, P. Vinoth, Mitigation of jamming attacks in wireless networks , .Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013.

[3] Anil Kumar Pinnaka, D. Tharashasank, V. S. K. Reddy," Cost performance analysis of intrusion detection system in mobile wireless ad-hoc network," Advance Computing Conference (IACC), 2013 IEEE 3rd International conference, 2013. pp.536 – 54.

[4] Mohit Soni, Manish Ahirwa, Shikha Agrawal," A Survey on Intrusion Detection Techniques in MANET ," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), ,2015, pp.1027-1032.

[5] S V Athawale, D N Chaudhari, Towards effective client-server based advent intrusion prevention system for WLAN," Computer, Communication and Control (IC4), 2015 International Conference, 2015, pp.1-5.

[6] Yujia Zhang, et al. An overview of wireless intrusion prevention systems , Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference, ,2010, pp.147-150.

[7] Open Source IDS / IPS / NSM engine . [Online]. Available: https://suricata-ids.org/

[8] Mohamed Elboukhari, et al. Intrusion Detection Systems in mobile ad hoc networks: A survey," Cryptography and Communication Systems (WCCCS), , 2014, pp.136-141.

[9] Khalid Alsubhi, et al., Performance analysis in Intrusion Detection and Prevention Systems," 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011), 2011, pp.369-376.

[10] Yaqing Zhang, Srinivas Sampalli, Client-based intrusion prevention system for 802.11 wireless LANs , 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications,2010, pp.100-107.

[11] http://www.cisco.com/c/en/us/products/collateral/wireless/adaptive- wireless-ips-software/data_sheet_c78-501388.html.

[12] S V Athawale, Dr M A Pund. ACIPS: Improvement of Client-Server based Intrusion Prevention System for Wireless LAN,International Journal of Innovative Research in Computer and Communication Engineering,(IJIRCCE)Vol. 5, Issue 4, ,2017, pp.6868-6871.

[13] S V Athawale1, M A Pund,Intrusion Prevention System for Wireless LAN Security: A Study, International Journal of Advanced Research in Computer and Communication Engineering,(IJARCCE),Vol. 5, Issue 10, 2016, pp.421-423.

[14] S V Athawale1, M A Pund,The Modern Approach in Wireless Intrusion Prevention System for Ad hoc Network: A Target Oriented Approach, International Journal of Advanced Research in Computer Science and Software Engineering,(IJARCSSE),Volume 7, Issue 2, 2017, p.1-7.

[15] S V Athawale1, M A Pund,A Novel Algorithm to Determine the Attacks Intention in Wireless Ad hoc Networks", International Journal Of Engineering And Computer Science, Volume 5 Issue 12, 2016, pp.19283-19287.

[16] S V Athawale1, M A Pund,"Comparative Performance Evaluation of Routing Protocols for Wireless Ad hoc

Network", International Journal of Innovative Research in Science,Engineering and Technology,(IJIRSET),Volume 6, Issue 10, 2017, pp.19411-19416,.

[17] S V Athawale1, M A Pund, Real-time Intrusion Prevention System to Increase Computer Security in Wireless LAN, nternational Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 5, Issue 9,,2017, pp.1428-1432.