IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 6 (Sep. - Oct. 2013), PP 53-59
www.iosrjournals.org

A Modular Approach To Intrusion Detection in Homogenous Wireless Network

Ajita Mishra[1], Ashish Kumar Srivastava[2]
[1]*(PG Scholar, CSE, NIIST Bhopal, India)*
[2]*(Associate Professor, CSE, NIIST Bhopal, India)*

Abstract: *Wireless network is the latest and popular technology nowadays. Due to its ample advantage in various fields, it has always been the prime target for hackers and attackers to break through its security and the number of attempts are growing day by day, so the need of real time monitoring and prevention system is required. There are so many methods to detect and prevent intrusion in wireless network but they lack in so many ways or are inefficient. This paper has an inclination to outline the fundamentals of intrusion detection in wireless network, describing the form of attacks and state the motivation for intrusion detection in wireless network and use the modular approach to detect intrusion in a wireless network. Then validation of proposed approach on real network data with analytical model for intrusion detection which allows us to analytically formulate intrusion detection possibility is done.*

Keywords - WNS, IDS, attacks, SID, WIPS

I. Introduction

Interest in wireless network security has been growing in recent years. Although several security-defense systems have been developed such as firewalls, encryption, authentication, and VPNs, most of the wireless systems are still susceptible to attacks. Unfortunately, complete attack prevention in wireless networks is not realistically attainable due to the openness of wireless medium, system complexity, configuration and administration errors, abuse by authorized users, lack of centralized monitoring and management points, dynamically changed network topologies, etc. The wireless network is a rapidly emerging new technology square measure. New applications square measure being developed like in traffic, setting observance, healthcare, military applications, home automation. A wireless network is susceptible to numerous attacks like jam, battery avoidance, routing cycle, Sybil, cloning. To protect Wireless network against completely different varieties of vulnerabilities, preventive mechanisms like cryptography and authentication will be applied to stop some sorts of attacks. Additionally, these mechanisms squares the measures which are effective to guard from outside attacks and didn't guarantee the interference of intruders from outside or within the network. Today Intrusion detection is used as a security resolution in a much wired networks within the type of software/ hardware by that one will sight unwanted services happening in the system by the approach of enhanced/abnormal network activity and determine suspicious patterns that will indicate whether or not the network/system is beneath attack? For Wireless network many schemes were projected however they need restricted options like a concern for attacks on a specific layer. A wireless IDS may aid within the detection of a variety of attacks. In an attempt to spot potential WAP targets, hackers ordinarily use scanning computer code. Hackers or curious people can use tools like Netstumbler or Kismat to plan a given area's WAPs.

Many types of wireless networks are used, they are following: Adhoc network [11] is a type of wireless network and decentralized in nature. It is a set of wireless mobile nodes forming a momentary network without any centralized access point. Decentralized nature of wireless ad hoc networks makes them suitable for multiple applications, where central nodes can't be relied on and may develop the scalability of networks as compared to wireless networks. Ad hoc network is also referred as IEEE 802.11 wireless networks. The ad - hoc network goes through a lot of issues, congestion and security are the major issues of current research, which leads to severe dilapidation of network throughput and increases the routing overheads. Mobile ad hoc networks (MANET) are an application of Adhoc networks. Another wireless network is Sensor Network. A wireless sensor network (WSN) [3] consists of spread autonomous sensors to monitor physical or environmental conditions, such as sound, temperature, pressure, etc. Intrusion detection in Wireless Sensor Network is of practical concern in many applications such as detecting an intruder in a battleground. Today such networks are used in many consumer and industrial applications, such as machine health monitoring, industrial process monitoring and control, traffic control resident application areas, environmental and local monitoring.

The rest of the paper is organized as follows. In the next section II we discussed about the IDS and classification of the IDS system. Explaination of various types of exiting attacks and intrusion detection techniques in section III. Our proposed work is discussed in section IV. Finally section V gives result and then section VI & VII includes future work and conclusion.

II. Intrusion Detection System (IDS)

An **Intrusion detection system (IDS)** is hardware and/or software designed to sense superfluous attempts at accessing, manipulating, and/or disabling of computer through a network, such as the Internet. These attempts may take the form of attacks like crackers, malware and/or dissatisfied employees. IDS indirectly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of nasty behaviors that can give and take the security and trust of a computer system. This comprises network attacks against data determined attacks on applications, host based attacks such as unauthorized logins and access to sensitive files, privilege escalation, susceptible services, and viruses.

Refers to the collaboration degree of IDS agents on the monitored system. Based on the IDS architecture, we differentiate between autonomous and distributed IDS systems.

1) Autonomous IDS: In autonomous IDS architecture, each network node operates independently and is responsible for detecting attacks on its own accord; there is no interaction between the network nodes. This architecture is more proper for the flat networks than for the multi-layered networks.

2) Distributed IDS: It comprises a number of network nodes which are responsible for collecting local audit data independently, and then collaboratively investigate it in a broader range in order to carry out a global IDS. This architecture is applicable for flat networks, and also for multilayered networks.

2.1 Detection Techniques

Detection techniques describe the detection manner. There are two complementary and one hybrid detection techniques to differentiate between the normal and malicious traffic.

1) Signature-based detection technique: It is also known as Misuse Detection. In this technique, IDS system inspects the monitored packets on the basis of detecting any facts of the attacks, according to a predefined and created model for specific known attacks. The advantage of this detection technique is its capability to detect instances of known attacks. The main disadvantage is the difficulty of gathering information about all current attacks, and thus this leads to the lack of the ability to detect the newly invented attacks as well as some variations of existing attacks, causing false negative.

Intrusion signatures have been characterized as a string, event sequences, graphs, and intrusion scenarios (consisting of target states, event sequences, and their preconditions). FSM (finite-state-machine), colored Petri Nets, associate roles and production rules of expert systems have been used to represent and recognize intrusion signatures. Intrusion signatures are either physically encoded or manually learned through data mining. But, signature recognition techniques have a limitation in that they cannot detect original intrusions whose signatures are unknown.

2) Anomaly-based detection technique: In this technique, the IDS system inspects the system activities on the basis of detecting any deviations from an established model of the normal and expected behavior through the system. This technique does not require a prior knowledge of attacks, and thus it can detect the new attacks. The main disadvantages are the disability to identify the attack type and the high false positive rate.

3) Specification-based detection technique: Combines the Advantages of signature-based detection and anomaly-based detection techniques. This arrangement detects unknown attacks, using the detection rate of anomaly detection, and accuracy of misuse detection. Consequently, it gets the targets of high detection rate and low false positive rate.

2.2 Requirements of IDS in Wireless Network

Any IDS should discover a considerable share of intrusions into the supervised system, whereas keeping the warning rate at a suitable level at a lower cost. It's expected that a perfect IDS is likely to support many of the subsequent needs :

- The IDS must not introduce a brand new weakness infrastructure. In the painter. That is, the IDS itself ought to not build a node weaker than it already is.
- Associate in Nursing IDS ought to run ceaselessly and stay transparent to the system and users.
- The IDS ought to use very little system resources as potential to observe and stop intrusions. IDS that needs excessive communication among nodes or run advance algorithms square measure not fascinating.
- It should be fault-tolerant with in the sense that it must be ready to pass though system crashes, hopefully recover to the previous state, and resume the operations before the crash.
- Excluding sleuthing and responding to intrusions, associate in Nursing IDS ought to conjointly resist subversion. It should monitor itself and observe if it's been compromised by the associate in Nursing offender.
- Associate in Nursing IDS ought to have a correct response. In other words, Associate in Nursing IDS must

not solely observe but conjointly answer detected intrusions, preferably while not human intervention.

- Accuracy of the IDS is another major consider MANETs. Fewer false positives and false negatives square measure desired.

2.3 Wireless Intrusion Prevention System

Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the existence of un-authorized access points , and can do automatic intrusion prevention. The main purpose of a WIPS is to prevent un-authorized network access to local area networks and other information resources by wireless devices. WIPS which is an extension of WIDS not only detects wireless intrusions, but also can prevent them.

2.4 Classification of Some Open-Source and Commercial Widss

WIDS	Detection Techniques	Information Source	Architecture	Respons e
SnortWirel ess	Signature-based	NIDS	Autonomous/ Distributed	Passive/ Active
WIDZ	Signature-based	NIDS	Distributed	Passive/ Active
AirMangne t	Signature-based /Anomaly-based	NIDS	Autonomous/ Distributed	Passive/ Active
AirDefence	Signature-based /Anomaly-based	NIDS	Distributed	Active
AirIDS	Signature-based /Anomaly-based	NIDS	Distributed	Active
Kismet	Signature-based	NIDS	Autonomous	Passive

III. Literature Review

There are various techniques implemented in the security of the wireless network and attacks that affect the security of wireless system, so researchers have proposed some of techniques to introduce the basics of the intrusion detection in Wireless network, the definition of the intrusion, kinds of intrusions/attacks in Wireless network, the motivation and want for intrusion detection and therefore the challenges of developing an honest intrusion detection theme for wireless network. The definition of the Intrusion/Attack: [4] defines the intrusion as any set of actions that try to compromise the most parts of the safety system: the integrity, confidentiality or handiness of a resource. Within the same work, the interloper so was outlined as a personal or a cluster of people who take the action within the intrusion. [5] Adds the statement of success or failures of those actions thus it additionally refers to the attacks against the PC system. Within the theme of wireless detector network, the conception is still constant since the intrusion additionally targets any of the parts mentioned above. The character of Wireless network and its special characteristics just like the harsh readiest, energy constraints and therefore the media of communication makes them terribly liable to the intrusions quite different networks. Following attacks occur in wireless network: [1]

- **Probing & Network Discovery:-**

Before an attacker is capable to attempt any kind of wireless harm one of the main activities would be for him to recognize the various wireless targets in range. This type of attack is described amongst the first activities engaged by any attacker. There are two types of probing- active and passive probing. Active probing involves the attacker actively sending probe needs with no SSID configured in order to request a probe reaction with SSID information and other information from any access points in range. Active probing cannot detect for access points that are covered or out of range of the attacker's wireless transmission range. When an attacker engages in passive probing, he/she is listening on all channels for all wireless packets being received and sent without sending even a single packet, thus the detection capacity is not limited by its transmission power. A superior example of a tool that uses active probing is NetStumbler and for passive probing, Wirehsark tool is used .

- **Surveillance:-**

Once the wireless aim has been recognized, the attacker can continue to gather information about the network using tools like airodump or kismet. The gathered data can be saved in pcap format for following offline analysis. If the traffic stream is not encrypted, directly the attacker could look at the traffic stream and recognize the network parameters (e.g. IP address range, gateway, MAC address, etc.) from the traffic. If the

traffic stream is WEP encrypted, there are WEP crackers which are available for him. Airodump is used to collect all the encrypted packets and aircrack is then used to crack the WEP key given if enough WEP are gathered.

- **DOS (Denial of Services) attack:-**

Denial Of Service (DOS) attack make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities.

- **Impersonation:-**

Another category of attacks that can be simply executed in a wireless network is the impersonation attack. In such an attack, the attacker adjusts his MAC address to a MAC address which he found prior during the surveillance state. This MAC address would most positively belong to an authorized client in the network. This is generally done to overcome the MAC filtering abilities of access points where only a list of authorized MAC addresses is allowed to use the wireless network. To adjust the MAC address manually in the windows, locate the registry settings for your wireless NIC and add a new string call network address with the new MAC address information to it.
Key fingerprint = AF19 FA27 2F94 998D FDB5 EE3D F8B5 06E4 A169 4E46

- **Man in the middle and Rouge AP:-**

In this type of attack, the attacker attempts to introduce himself in the middle of a communication for purposes of catching client's data and could potentially adjust them by discarding them or sending them out to the real target.
Man-in-the-middle attack is also known as:

- ✓ Bucket-brigade attack
- ✓ Fire brigade attack
- ✓ Monkey-in-the-middle attack

In order to insert oneself in the middle of the communication, one has to achieve two tasks, first, the suitable AP allocates the client must first be brought down or made "extremely hard" so as to create a "complex to connect" scenario for the wireless client. Secondly, the attacker must set up an interchange rouge AP with the same records as the original, for purposes of allowing the client to connect to it. With the fast development of wireless network, the problems on wireless security have become more and more prominent. And the technologies of firewall and intrusion detection cannot solve these problems satisfactorily. However, wireless intrusion prevention systems which can prevent attacks for WLAN excellently have become the research hotspot. We propose a common wireless intrusion prevention framework (CWIPF), and describe some key technologies used in this framework. Finally, we proposed some study issues should be focused on in the future. Index Terms-intrusion prevention, wireless LAN, CWIPF, network security [2].

The increasing confidence upon wireless networks has put tremendous emphasis on wireless network security. Intrusion detection in wireless network has become an essential component of any helpful wireless network security system, and has recently gained attention in both research and industrial communities due to widespread use of wireless local area network (WLAN). Although some intrusion prevention systems have recently appeared in the market, their intrusion detection capabilities are limited. This paper focus on detecting intrusion or anomalous behavior of nodes in WLAN's Using a modular technique. We explore the security vulnerabilities of 802.11, numerous intrusion detection techniques, and different network traffic metrics also called as features. Based on the study of metrics, proposed a modular based intrusion detection approach. [3]

Intrusion detection in Wireless Sensor Network (WSN) is of useful attention in various applications such as detecting an intruder in a battlefield. The intrusion detection is a mechanism for a WSN to detect the existence of improper, inaccurate, or anomalous moving attackers. In this paper, we have considered the issue according to heterogeneous WSN models. Furthermore, we have considered two sensing detection models: single-sensing detection and multiple-sensing detection. [4]

[19] In this paper, a novel framework to detect wireless network attacks based on anomaly analysis of the behavior of wireless networks and data mining techniques. WSPS approach is based on multi-channel online monitoring and anomaly analysis of device localization, frame behavior, and network access violations with respect to multiple-observation time windows. Using wireless network resources, WSPS produces network features, wireless-network-state machine violations, and generates wireless network flows (WNetFlows) for multiple time windows, and utilize the dynamically renewed anomaly and misuse rules to identify complex known and unknown wireless attacks and take appropriate proactive actions.

[20] In this paper, propose a separation table to detect intrusion in hierarchical wireless sensor networks and to approximate the effect of intrusion detection effectively. The primary experiment shows that the isolation table can detect and prevent intrusion's attacks effectively. But this method is not good enough to detect anomaly using IDS.

IV. Proposed Methodology

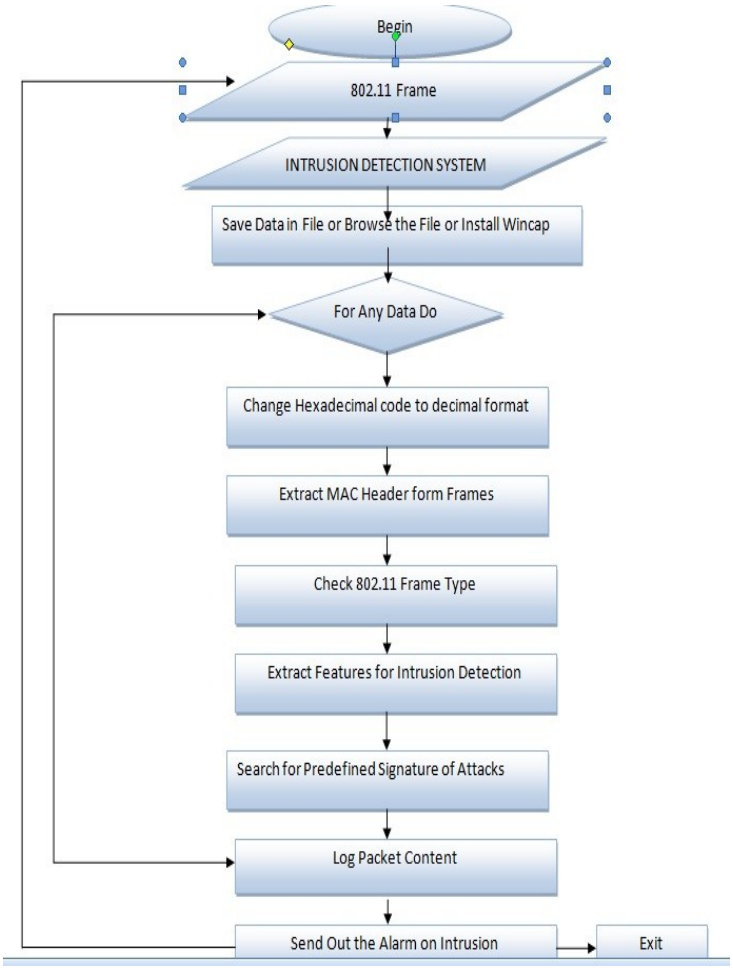
In our approach, cluster the wireless traffic data and then use the heuristic function to make each instance intrusive or normal. The heuristic function is used in the execution of modules for individual features in intrusion detection system. In which we search for the specific features collectively defined an activity (i.e. Pattern) followed by an attack. Then we put these results of features in a table consist list of features with respect to MAC or IP address of a node (i.e. We maintain a check list for individual node), so we can calculate the intrusive behavior of a node rather than a particular attack. A technique adopted for the detection of features is tabular in which create a list of features vertically and on the basis of detecting features the alarm can be generated for the respective attacks. It is a reverse approach than the usual Intrusion Detection Systems in which they detect specific attacks. In the earlier IDS, two checks were needed for the same feature in two different attacks but in proposed Modular Approach there is only a single check required to detect same feature in both attacks. The following steps are followed to implement modular approach for intrusion detection in wireless environment:

- Generate algorithm to implement modular approach.
- Collecting knowledge of signature of attacks used in wireless networks.
- Capture database of wireless network.
- Implement approach in system compatible platform.

A Novel Solution for Intrusion Detection & Prevention.

1. Begin
2. Sniff for 802.11 frames.
3. Save data in a file that can be accessed through the system and in the required format.
4. Open file contains data of the network
   - 4.1. Change hexadecimal code in decimal format
   - 4.2. Purse frames and extract MAC headers from the frames
   - 4.3. Check 802.11 frame types.
   - 4.4. The extract feature requires to detect intrusion
   - 4.5. Search for the predefined signature of attacks in the database
5. Log packet content
6. Send out an alarm if intrusion found (i.e. Signature match)
7. Analysis data packet with isolated from (Analysis illegal behaviors).
8. Save all the intrusion data in the event database.
9. Set working Frequency of monitoring channel.
10. Exit and Repeat

Algorithm for Intrusion Detection & Prevention

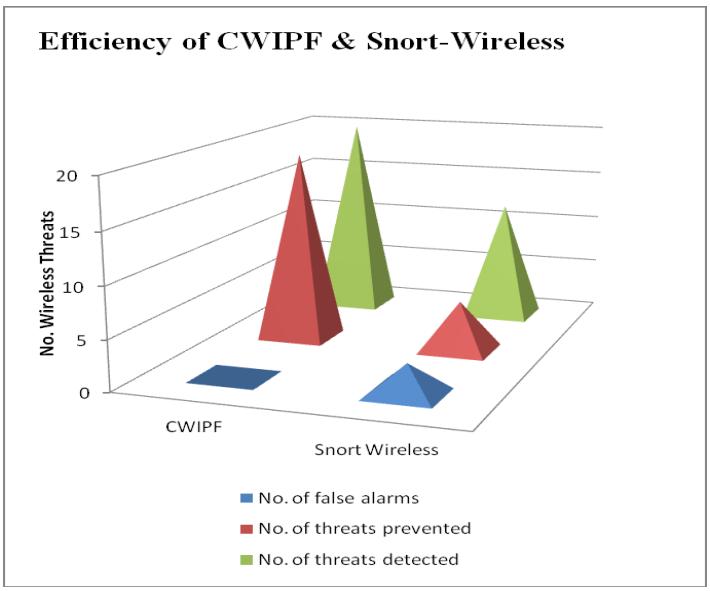


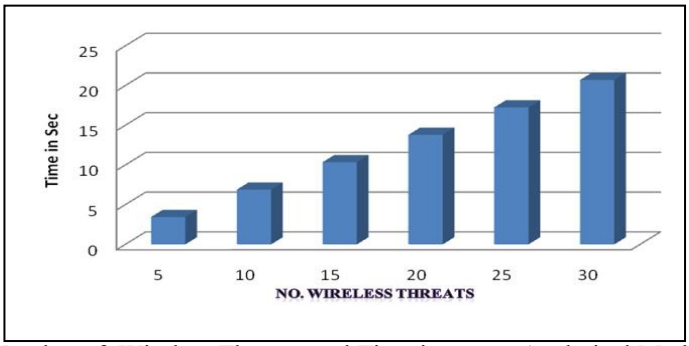
Flow Chart

As discussed above SID and AID both have problems of higher false alarm rate due to inappropriate threshold value to generate alarms for intrusion. An approach is needed that uses the combination of both of these techniques. In modular approach we are using the signature based detection approach by detecting the feature listed for known attacks as well as for checking the abnormal behavior through a table of feature detected so we can detect the unknown attacks. During algorithm design we take care of the following basic terminologies of modular approach that can detect known as well as unknown attacks. Because that system is designed to implement for wireless network one more thing that is crucial to remember is that it should not increase the CPU overhead more than 5-6%. In this method Intrusion detection system starts with 802.11 Frame thereafter it look for format (Given format) to decide whether a particular file is intruders file or not. For that to any given data change Hexadecimal to decimal format thereafter extract the MAC header from the frame then compare with 802.11 Frame type and extract intrusion detection from features with given predefined signature attacks. Then with this required log file is open with shows the no of intruders in this file. Send out the alarm if intrusion is detected such process is applied to every upload file.

V. Result

We have design and implement the CWIPF with Snort-wireless. We have created evaluating experiments, based on the performance of CWIPF with Snort-Wireless. In our experiment,twenty wireless threats square measures launched against the WLAN, together with DoS, MAC spoofing, MITM, rogue AP, misconfigured AP attacks.When CWIPF is applied on 20 threats file then it detect 19 threats file which can prevent attackers from damaging wireless networks. Snort-Wireless prevents only 5 threats out of detected 12 threats. Moreover, Snort-Wireless extracted three false alarms.The figure shows the efficiency of these two WIPS at detecting and preventing wireless threats.





Number of Wireless Threats and Time in sec an Analytical Model.

VI. Future Work

In this research wireless intrusion detection and preventionthe algorithm has been developed which shows to be effective in detection and prevention of intrusions. The intrusion detections are applied in internet application and parallel computer interconnection network. The Algorithm can be extended and compare with real time work such as WEKA tools.

VII. Conclusion

This paper examines the intrusion detection problem by characterizing intrusion detection possibility with respect to the intrusion distance and the network parameters like sensing range, node density and transmission range. The analytical model for intrusion detection allows us to analytically formulate intrusion detection possibility within an assured intrusion distance under various application scenarios and then validate our approach on real network data in which a a database of 20 files is used and then successfully detect the signature that are provided in our experiment. Our result shows the name of application and port of the system using that application, so it can be possible to punish that system if the system is designed to do that.

References

[1] A. Mishra, A.K. Srivastava, "A Survey on intrusion Detection System for Wireless Network", IJCA, vol. 73- No.21, pp. 37-40 July 2013.

[2] Y. Zhang, G. Chen, W. Weng, and Z. Wang, "An Overview of Wireless Intrusion Prevention Systems,"*IEEE ICCSNA* , vol. 3, no. 12, pp. 147–150, 2010.

[3] T. Badal, D. Verma, "A Modular Approach for Intrusion Detection System in Wireless Networks", *IJACNS*, vol. 1, pp. 57-61, 2011, ISSN:2250-3757.

[4] K. Suresh, A. Sarala Devi, and Jammi Ashok, "A Novel Approach Based Wireless Intrusion Detection System", *IJCSIT*, Vol. 3 (4) , 2012,4666 – 4669, ISSN:0975-9646.

[5] Heady, R., "The Architecture of a Network-level Intrusion Detection System."1st Edn., Department of Computer Science, Mexico, pp: 18, 1990.

[6] Zamboni, D., 2001. Using internal sensors for computer intrusion detection. Purdue University.

[7] Debar, H. M. Dacier and A. Wespi, 1999. Towards at taxonomy of intrusion-detection systems. Comput. Netw., 31: 805-822.

[8] S. Zhong, T. M. Khoshgoftaar and S. V. Nath, "A Clustering Approach to Wireless Network Intrusion Detection", in proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAL'O5), PP. 54-60, 2005.

[9] V. Gupta and S. Gupta, "Experiments in Wireless Internet Security", Wireless Communications and Networking Conference, (WCNC 2002), IEEE Volume 2, pp. 860-864, 2002.

[10] Z. Li, A. Das and J. Zhou, "Theoretical basis for intrusion detection," Information Assurance Workshop, (IAW 2005), proceedings from the sixth Annual IEEE SMC, pp. 184-192, 2005.

[11] Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava, "Intrusion Detection: A Survey", Managing Cyber Threats: Issues, Approaches and Challenges, Vol. 5, 2005, Springer Publisher.

[12] P. Brutch and C. Ko, "Challenges in intrusion detection in wireless ad-hoc networks,"IEEE Proceedings of Workshop on Security and Assurance in Ad hoc Networks, 2003, pp368 - 373, Jan. 2003.

[13] Tsakountakis, G. Kambourakis, S. Gritzalis, "Towards effective Wireless Intrusion Detection in IEEE 802.11i," in: Security, Privacy and Trust in Pervasive and Ubiquitous Computing, (SECPerU 2007), Third International Workshop, pp. 37-42, 2007.

[14] N. Ye, SM. Emran, Q. Chen and S. Vilbert,"Multivariate statistical analysis of audit trails for host-based intrusion detection", Computers, IEEE Transactions on Volume 51, Issue 7, pp. 810 – 820, July 2002.

[15] El-Khatib, Khalil. "Impact of feature reduction on the efficiency of wireless intrusion detection systems." Parallel and Distributed Systems, IEEE Transactions on 21, no. 8 (2010): 1143-1149

[16] Tao, Zhiqi, and A. B. Ruighaver. "Wireless intrusion detection: Not as easy as traditional network intrusion detection." In *TENCON 2005 2005 IEEE Region 10*, pp. 1-5. IEEE, 2005.

[17] Khoshgoftaar, Taghi M., Shyam Varan Nath, Shi Zhong, and Naeem Seliya. "Intrusion detection in wireless networks using clustering techniques with expert analysis." In Machine Learning and Applications, 2005. Proceedings. Fourth International Conference on, pp. 6-pp. IEEE, 2005.

[18] Yang, Yatao, Ping Zeng, Xinghua Yang, and Yina Huang. "Efficient intrusion detection system model in wireless mesh network." In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on, vol. 2, pp. 393-396. IEEE, 2010.

[19] Fayssal, Samer, Youssif Alnashif, Byoung Kim, and Salim Hariri. "A proactive wireless self-protection system." In Proceedings of the 5th international conference on Pervasive services, pp. 11-20. ACM, 2008.

[20] Chen, Rung-Ching, Chia-Fen Hsieh, and Yung-Fa Huang. "A new method for intrusion detection on hierarchical wireless sensor networks." In Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, pp. 238-245. ACM, 2009.

[21] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Comm.,vol. 11, no. 2, 2004