# Intrusion Detection System: A Review

Swati Gupta[1]
Assistant Professor,
Vaish College of Engineering, Rohtak

Radhika Garg[2]
Assistant Professor,
Vaish College of Engineering, Rohtak

***Abstract:*** **Intrusion Detection System which is also known as IDS has been reviewed with its pros and cons. The demand of different smart devices such as laptops, smart phones are increasing to gain network connectivity vastly. Therefore numerous companies have begun to work on means in order to accomplish this task. There are several researchers in past in which different IDS model and their working has been discussed. But these researches have their own limitations. This paper discusses different types of IDS technologies such as Network Based IDS, Wireless IDS, Network Behavior Anomaly Detection, Host Based IDS etc. More over need of IDS and issues faced during its use has been explained in this review paper.**

***Keywords: Network security, IDS, Mobile Computing Devices***

## INTRODUCTION

Nowadays use of mobile computing devices is increasing day by day. The demand of different smart devices such as laptops, smart phones are increasing to gain network connectivity. Therefore several groups started working on means to accomplish this task. Therefore standard is available, one with presence of a base station and other without presence of a base station. In latter case computers would companies to each other directly. It could be define as an ad-hoc network.

Fig1 Mobile Computing Devices

As awareness now that MANETs do not have a fixed topology, thus every single node in network acts as a host as well as a packet forwarding device i.e., a router. Additional, nodes related to an network could be transferred in required direction. These are enabling to different nodes to leave network at any point of time. A further specified case of ad-hoc networks is when nodes i.e., computers in this case are mobile. In situations, each node consists of a host and a router on same device. Mean to say that nodes form a network having no any use of an external routing device. When a number of these nodes happen to be near to each other and form networks. It is known as ad-hoc network or Mobile ad hoc network (MANET).

## [2] LITERATURE SURVEY

There are several researchers in past in which IDS and it working has been discussed. These are considered here such as:

**Nilotpal Chakra borty (2013)** discussed intrusion detection system and intrusion prevention system. They also provided a comparative study in their research work. As awareness now that MANETs do not have a fixed topology, thus every single node in network acts as a host as well as a packet forwarding device i.e., a router.

**Besant's Kumar(2013)** analyzed Intrusion Detection System- Types and Prevention. [2] Nowadays use of mobile computing devices is increasing day by day. The demand of different smart devices such as laptops, smart phones are increasing to gain network connectivity. Therefore several groups started working on means to accomplish this task

**Dr. S.Vijayarani (2015)** explained intrusion detection system. They discussed that IDS is a software application. It is able to monitor or control network or system activities. It has been used to search any type of malicious operations. Tremendous growth as well as usage related to internet increases. These techniques are used to secure as well as communicate digital information in a safe manner. Therefore, hackers use several kind attacks to get important. Several intrusion detection mechanisms, methods as well as algorithms enable to capture such attacks.

**Nilotpal Chakra borty(2013)** evaluated intrusion detection system and intrusion prevention system. **They provide review on this concept. In research work,** IDS that is a software application, is used frequently to control network or system activities. It has been used to search any type of malicious operations. Tremendous growth along with usage related to internet increases.

## [3] DIFFERENT INTRUSION DETECTION SYSTEM

There are many types of IDS technologies. These techniques are differentiated on base of type of events in which these are monitored. The ways in which, these are used is also considered.

1. Network Based IDS
2. Wireless IDS
3. Network Behavior Anomaly Detection
4. Host Based IDS

### *1. NETWORK BASED IDS*

Network based IDS (NIDS) are used to detect network traffic. It is required for a particular network segment. These are used to analyze network and activity of application protocol. It is made in order to identify suspicious activity. Commonly, it is deployed at a boundary between networks such as in routers, firewalls, virtual private networks etc.

### *2. WIRELESS IDS*

It is similar to Network based IDS (NIDS) which is applicable to analyze network traffic. Therefore, in future, it would be able to analyze wireless-specific traffic, including scanning for external users. It has been used when one tries to make connection to access points (AP), rogue APs, users outside physical area of company etc. As networks gradually more support wireless technologies at several points related to a topology, it would be efficient to play larger roles in security.

### *3. NETWORK BEHAVIOR ANOMALY DETECTION*

This type of detection mechanism is utilized to view traffic on network segments. It is required to decide anomalies appear in traffic. Usually Segments see very little traffic or segments that see only specific traffic could send amount or type of traffic in condition of any appearance of any unwanted event. This type of detection system uses different sensors in order to generate a good snapshot related to any network. Therefore it requires benchmarking and base lining. These are used to decide nominal amount related to traffic of segment.

### *4. HOST BASED IDS*

In this technology, installation of software agents is made. It is situated on each of computer hosts related to network. This task is performed to monitor events happening within that host only. HIDS is able to analyze network traffic and system-specific settings. Commonly, HIDS are used on critical hosts for example publicly accessible servers and servers having important data or content.

## [4] NEED OF INTRUSION DETECTION SYSTEM

The need of Intrusion Detection System has been discussed in this section

**They Can Be Tuned to Specific Content in Network Packets:** Firewalls might be able to show you ports and IP addresses that are used between two hosts, but in addition a NIDS could be tuned to show you specific content within packets. This could be used to for uncovering intrusions such as exploitation attacks or compromised endpoint devices that are part of a botnet.

**They Can Look at Data in Context of Protocol:** When an NIDS performs protocol analysis, it looks at TCP and UDP payloads. The sensors could detect suspicious activity because they know how protocols should be functioning.

**They Can Qualify and Quantify Attacks:** An IDS analyzes amount and types of attacks. This information could be used to change your security systems or implement new controls that are more effective. It could also be analyzed to identify bugs or network device configuration problems. The metrics could then be used for future risk assessments.

**They Make It Easier to Keep Up With Regulation:** Because an IDS gives you greater visibility across your network, they make it easier to meet security regulations. You could also use your IDS logs as part of documentation to meet certain requirements.

**They Can Boost Efficiency:** Because IDS sensors could detect network devices and hosts, they could inspect data within network packets and identify services or operating systems that are being utilized. This saves a lot of time when compared to doing it manually. An IDS could also automate hardware inventories, further reducing labor. These improved efficiencies could help to reduce an organization’s staff costs and offset cost of implementing IDS.

## [5] ISSUES

The issues faced by IDS have been explained in this section:

**They Will Not Prevent Incidents By Themselves:** An IDS does not block or prevent attacks, they merely help to uncover them. IDS need to be part of a comprehensive plan that includes other security measures and staff who know how to react appropriately.

**An Experienced Engineer Is Needed to Administer Them:** An IDS is immensely helpful for monitoring network, but their usefulness all depends on what you do with information that they give you. Because detection tools don’t block or resolve potential issues, they are ineffective at adding a layer of security unless you have right personnel and policy to administer them and act on any threats.

**They Do Not Process Encrypted Packets:** An IDS cannot see into encrypted packets, so intruders could use them to slip into network. An IDS would not register these intrusions until they are deeper into network, which leaves your systems vulnerable until intrusion is discovered. This is a huge concern as encryption is becoming more prevalent to keep our data secure.

**IP Packets Can Still Be Faked:** The information from an IP packet is read by an IDS, but network address could still be spoofed. If an attacker is using a fake address, it makes threat more difficult to detect and assess.

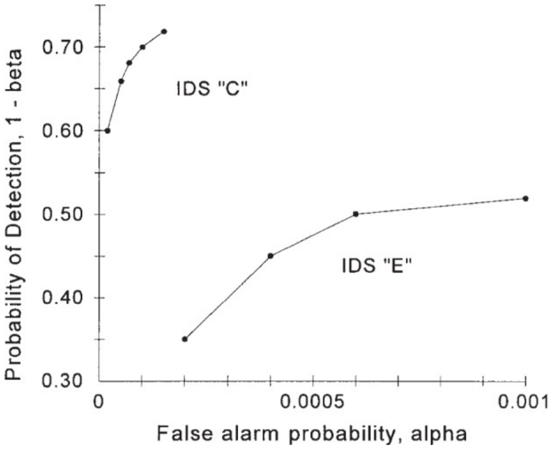
**False Positives Are Frequent:** One significant issue with an IDS is that they regularly alert you to false positives. In many cases false positives are more frequent than actual threats. An IDS could be tuned to reduce number of false positives, however your engineers would still have to spend time responding to them. If they don't take care to monitor false positives, real attacks could slip through or be ignored.

**They Are Susceptible to Protocol Based Attacks:** An NIDS analyzes protocols as they are captured, which means that they face same protocol based attacks as network hosts. An NIDS could be crashed by protocol analyzer bugs and also invalid data.

**The Signature Library Needs to Be Continually Updated to Detect Latest Threats:** An IDS is only as good as its signature library. If it isn't updated frequently, it won't register latest attacks and it can't alert you about them. Another issue is that your systems are vulnerable until a new threat has been added to signature library, so latest attacks would always be a big concern.

## [6] EVALUATION

A computer intrusion detection system is concerned with recognizing whether an intrusion is being attempted into a computer system. An intrusion detection system is providing some type of alarm to represent its assertion that an intrusion is present. The alarm might be correct or incorrect. A decision maker could decide to respond to alarm or to ignore the alarm. This section is explaining a decision analysis mechanism for determining the best operating point for an IDS and an expected cost metric that can be used to evaluate an IDS. An IDS's receiver operating characteristic (ROC) curve describes the relationship between the two operating parameters of the IDS, its probability of detection, 1−β, and its false alarm probability, α. That is, the ROC curve displays the 1−β provided by the IDS at a given α. It also displays the α provided by the IDS at a given 1−β. The ROC curve thus summarizes the performance of the IDS. We do not address how one generates this ROC curve, just what to do with it after it is determined



**.Fig 2** Two possible ROC curve

Above figure shows two possible ROC curves that have been used. These are similar to two ROC curves that were confirmed from actual data in 1998 DARPA off-line intrusion detection evaluation. IDS E's ROC curve is found similar to ROC curve for EMERALD and IDS C's ROC curve is similar to ROC curve for the Columbia IDS. IDS "C" is shown with five discrete operating points, and IDS "E" is shown with four. The lines shown connecting points are added as a visual aid to the reader but are irrelevant to describing performance of IDSs.

## [7] CONCLUSION

Differ from existing approaches related to dynamic tainting; our technique is based on positive tainting, which explicitly identifies trusted data in a program. In research paper, problem of false negatives is eliminated that might result from incomplete identification of all untrusted data sources. False positives, although possible in some cases, could typically be easily eliminated during testing. In IDS system, a data transmission mechanism is established to send and receive packets.

## REFERENCES

[1] Nilotpal Chakra borty(2013) "intrusion detection system and intrusion prevention system: a comparative study" International Journal of Computing and Business Research (IJCBR) Volume 4 Issue 2 May 2013 B.Santos Kumar(2013) "Intrusion Detection System- Types and Prevention" International Journal of Computer Science and Information Technologies, Vol. 4 (1),2013

[2] Dr. S.Vijayarani (2015) "INTRUSION DETECTION SYSTEM – A STUDY" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[3] 3E. Ahmed, K. Samad, and W. Mahmood, "Cluster-based intrusion detection (cbid) architecture for mobile ad hoc networks," in 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Proceedings, 2006.

[4] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in Wireless Network Security, pp. 159–180, Springer, 2007.

[5] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in Applications and Internet Workshops, 2003. Proceedings. 2003 Symposium on, pp. 368–373, IEEE, 2003.

[6] M. Ngadi, A. H. Abdullah, S. Mandala, et al., "A survey on manet intrusion detection," International Journal of Computer Science and Security, vol. 2, no. 1, pp. 1–11, 2008.

[7] A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," 2012.

[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.

[9] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications,IEEE, vol. 14, no. 5, pp. 56–63, 2007.

[10] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in manet," in The 21st annual conference for information systems educators (ISECON), Rhode Island, USA, pp. 4–7, 2004.

[11] L.Bononi and C. Tacconi, "A wireless

intrusiondetection system for secure clustering and routing in ad hoc networks," in Information Security, pp. 398– 414, Springer, 2006.

[12] Z. Xing, L. Grunewald, and K. Phang, "A robust clustering algorithm for mobile ad- hoc networks," Handbook of Research on Next Generation Mobile Networks and Ubiquitous Computing, pp. 187–200, 2008.

[13] B. Kisku and R. Datta, "An energy efficient scheduling scheme for intrusion detection system in mobile ad-hoc networks," in Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, pp. 1–6, IEEE, 2012.