Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey over Recent Intrusion Detection Systems

Poonam Choubey, Priyanka Vijayavargiya
Computer Science & RGPV University
Madhya Pradesh, India

Abstract: The intrusion detection techniques using data mining have attracted more and more interests in recent years. As an important application of data mining these techniques aim to meliorate the great burden of analyzing huge volumes of audit data and realizing performance optimization of detection rules. In this paper, we have proposed a novel method for intrusion detection. The proposed intrusion detection is based on the acknowledgement based system.

Keywords: HIDS, IDS, AACK

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multi hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration.

The field of intrusion detection has received increasing attention in present years. First reason is the explosive growth of the internet and the large number of networked systems that exist in all types of organizations.

Because they only scrutinize network traffic [1] the NIDS do not benefit from running on the host. They are often run on dedicated machines that observe the network flows sometimes in conjunction with a firewall. In this case they are not affected by security vulnerabilities on the machines they are monitoring. Only a limited number of information can be inferred from data gathered on the network link. The widespread adoption of end-to-end encryption further limits the amount of information that can be gathered at the network interface.

One major shortcoming of NIDS is that they are oblivious to local root attacks. The authorized user of the system that attempts to gain additional privileges will not be deleted if attack is performed locally. The authorized user of the system may be able to set up an encrypted channel when accessing the machine remotely.

The HIDS have an ideal vantage point [6]. An HIDS runs on the machine it monitors, HIDS can theoretically observe and log any event occurring on the machine. The complexity of current operating system often makes it difficult if not impossible to accurately monitor certain events. There are many difficulties faced by security tools that rely on system calls interposition to monitor a host.

II. RELATED WORK

In this paper [1] the author has we discussed the security issues and their current solutions in the mobile ad hoc network. The nature of the mobile ad hoc network is vulnerable. The *ad hoc network [2]* is a collection of wireless mobile computers or nodes. The individual nodes in the mobile ad hoc network cooperate to each other by forwarding packets. It helps them in increasing their range. The work in [3] defined the Mobile Ad hoc Network of Networks as a group of large autonomous wireless nodes. All such nodes communicates with each other These nodes communicates on a peer-to-peer basis in a heterogeneous environment with no predefined infrastructure. Authors of paper [4] proposed a protocol for routing data in the ad hoc network. This work is based on dynamic source routing. This proposed protocol has the ability to adopt according to the routing changes. In paper [5], the author has developed model. This model is based on the sequential probability ratio. This test identifies the misbehaving nodes. It categorizes the routes in two categories: one which contains the jamming nodes & one which does not contain jamming nodes.

By definition, Mobile Ad hoc NET work (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

III. DISADVANTAGES OF EXISTING SYSTEM

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

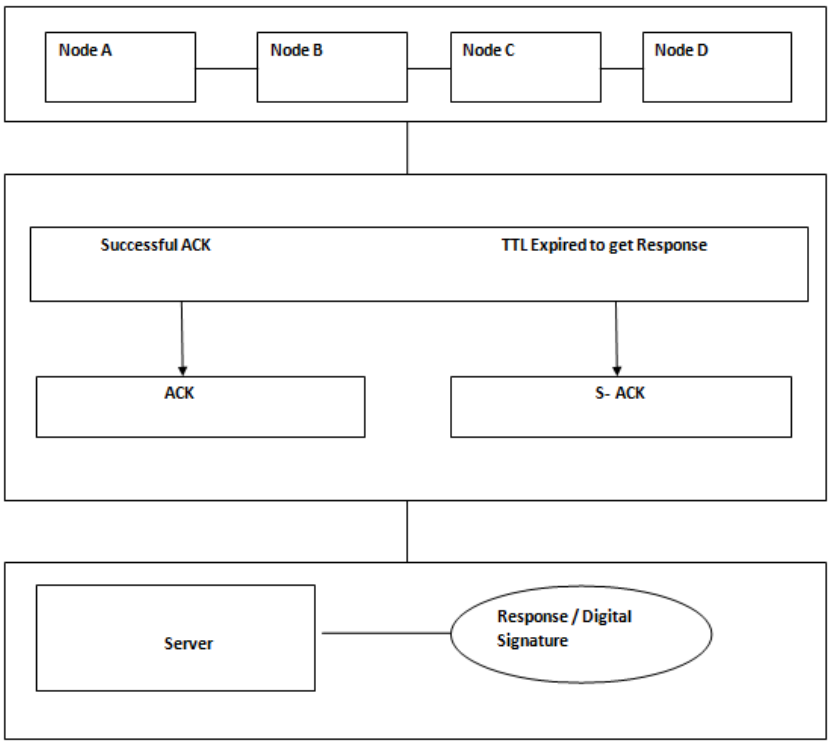
The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

IV. PROPOSED SYSTEM

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

SYSTEM ARCHITECTURE



ADVANTAGES OF PROPOSED SYSTEM

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.

V. CONCLUSION

In this paper, one novel method for the intrusion detection has been proposed. The proposed method is based on the concept of acknowledgement. We have analyzed the existing intrusion detection systems. We can conclude that many of the current intrusion decision system are signature-based systems. The SIDS or signature based IDS are also known as misuse detection looks for a specific signature to match or signaling an instruction. They are provided with the signatures or patterns, but SIDS are of little use for as yet unknown attack methods. It means that an IDS using misuse detection will only detect known attacks .

REFERENCES

[1] G. Jayakumar and G. Gopinath. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. In Journal of Computer Science 3(8): 574-582, 2007

[2] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012 – here1

[3] R.H. Akbani, S. Patel, D.C. Jinwala. "DoS Attacks in Mobile Ad Hoc Networks: A Survey", the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here1

[4] T. Anantvalee and J. Wu. A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer, 2008.

[5] L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

[7] V. C. Gungor, G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approac," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 42584265, Oct 2009.

[8] Y. Hu, D. Johnson and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.

[9] Y. Hu, A. Perrig, and D. Johnson. ARIADNE: A Secure OnDemand Routing Protocol for Ad hoc Networks. In the Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, Atlanta, GA, 2002.

