An Effective Study on Intrusion Detection in Wireless Ad-Hoc Networks

[1*]CH. G. V. N. Prasad, [2]Dr Deepak Kumar Verma
[1]Research Scholar, Department of CSE, Chhatrapati Shahu Ji Maharaj University, Kanpur
[2]Professor, Department of CSE, Chhatrapati Shahu Ji Maharaj University, Kanpur

ABSTRACT: Ad hoc networks networks have been serving us in for sure, for a considerable length of time, through their huge assortment of applications in greater part fields. Because of their elements like threatening arrangements, elevated degree of versatility, restricted assets and actual uncertainty, they are in cutting edge to assailants. First line of protection (cryptographic procedures, fire walls and so forth) shuts down these assaults. As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. How to do it differently and effectively is a challenging research problem. In this paper, we first examine the vulnerabilities of a wireless ad-hoc network, the reason why we need intrusion detection, and the reason why the current methods cannot be applied directly. We then describe the new intrusion detection and response mechanisms that we are developing for wireless ad-hoc networks.

Keywords: Ad-Hoc Networks, Intrusion Detection.

Article Submitted: ***April-2019;*** *Accepted:* ***July-2019;*** *Published:* ***October-2019***

INTRODUCTION

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays.

Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band, and follow the same hopping sequence or spreading code. The data-link-layer functions manage the wireless link resources and coordinate medium access among neighboring nodes. The medium access control (MAC) protocol is essential to a wireless ad-hoc network because it allows mobile nodes to share a common broadcast channel.

The network-layer functions maintain the multi-hop communication paths across the network; all nodes must function as routers that discover and maintain routes to other nodes in the network. Mobility and volatility are hidden from the applications so that any node can communicate with any other node as if everyone were in a fixed wired network. Applications of ad-hoc networks range from military tactical operations to civil rapid deployment such as emergency search-and-rescue missions, data collection/sensor networks, and instantaneous classroom/meeting room applications. The nature of

wireless ad-hoc networks makes them very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders a wireless ad-hoc network susceptible to attacks ranging from passive eavesdropping to active interfering.

Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad hoc network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly. Second, mobile nodes axe autonomous units that are capable of roaming independently.

This means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked. Since tracking down a particular mobile node in a large scale ad-hoc network cannot be done easily, attacks by a compromised node from within the network are far more damaging and much harder to detect. Therefore, any node in a wireless ad-hoc network must be prepared to operate in a mode that trusts no peer.

Third, decision-making in ad-hoc networks is usually decentralized and many ad-hoc network algorithms rely on the cooperative participation of all nodes. The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms. For example, the current MAC protocols for wireless ad hoc networks are all vulnerable. Although there are many MAC protocols, the basic working principles are similar.

In a contention-based method, each node must compete for control of the transmission channel each time it sends a message. Nodes must strictly follow the pre-defined procedure to avoid collisions or to recover from them. In a contention free method, each node must seek from all other nodes an 11nanimous promise of an exclusive use of the channel resource, on a one-time or recurring basis. Regardless of the type of MAC protocol, if a node behaves maliciously, the MAC protocol can break down in a scenario resembling a denial-of-service attack. Although such attacks are rare in wired networks because the physical networks and the MAC layer are isolated from the outside world by layer-3 gateways/ firewalls, every mobile node is completely vulnerable in the wireless open medium. Ad-hoc routing presents vulnerability. Most ad-hoc routing protocols are also cooperative in nature [14].

Unlike with a wired network, where extra protection can be placed on routers and gateways, an adversary who hijacks an ad-hoc node could paralyze the entire wireless network by disseminating false routing information. Worse, such false routing information could result in messages from all nodes being fed to the compromised node. Intrusion prevention measures, such as encryption and authentication, can be used in ad-hoc networks to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes. which carry the private keys? Integrity validation using redundant information (from different nodes), such as those being used in secure routing [16, 17], also relies on the trustworthiness of other nodes, which could likewise be a weak link for sophisticated attacks. The history of security research has taught us a valuable lesson - no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in. Intrusion detection presents a second wall of defense and it is a necessity in any high survivability network. In summary, a wireless ad-hoc network has inherent vulnerabilities that are not easily preventable.

To build n highly secure wireless ad-hoc network, we need to deploy intrusion detection and response techniques, and further research is necessary to adapt these techniques to this new environment, from their original applications in fixed wired network. In this paper, we propose our new model for intrusion detection and response in mobile, ad-hoc wireless networks. We are currently investigating the use of cooperative statistical anomaly detection models for protection from attacks on ad-hoc routing protocols, on wireless MAC protocols, or on wireless applications and services. We are integrating them into a cross-layer defense system and are investigating its defectiveness, efficiency, and scalability.

BACKGROUND OF INTRUSION DETECTION

As network-based computer systems play increasingly vital roles in modern society, they have become the targets of our enemies and criminals. When an intrusion (defined 3.5 "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [4]) takes place, intrusion prevention techniques, such as encryption and authentication (e.g., using passwords or biometrics), are usually the first line of defense. However, intrusion prevention alone is not sufficient because as systems become ever more complex, while security is still often the after-thought, there are always exploitable weaknesses in the systems due to design and programming errors, or various "socially engineered" penetration techniques (as illustrated in the recent "I Love You" virus). For example, even though they were first reported many years ago, exploitable "buffer overflow" security holes, which can lead to an unauthorized root shell, still exist in some recent system softwares. Furthermore, as illustrated by recent Distributed Denial-of-Services (DDOS) attacks launched against several major Internet sites where security measures were in place, the protocols and systems that are designed to provide services (to the public) are inherently subject to attacks such as DDOS. Intrusion detection can be used as a second wall to protect network systems because once an intrusion is detected, e.g., in the early stage of a DDOS attack, response can be put into place to minimize damages, gather evidence for prosecution, and even launch counter-attacks.

The primary assumptions of intrusion detection are: user and program activities are observable, for example via system auditing mechanisms; and more importantly, normal and intrusion activities have distinct behavior. Intrusion detection therefore involves 2apturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. Based on the type of audit data used, intrusion detection systems (IDSs) can be categorized as network-based or host-based. A network-based IDS normally runs at the gateway of a network and "captures" and examines network packets that go through the network hardware interface. A host-based IDS relies on operating system audit date to monitor and analyze the events generated by programs or users on the host. Intrusion detection techniques can be categorized into *misuse detection* and *anomaly detection.*

Misuse detection systems, e.g., IDIOT [8] and STAT [5], use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. For example, a signature rule for the "guessing password attack" can be "there are more than 4 failed login attempts within 2 minutes". The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the truly innovative (i.e., newly invented) attacks.

Anomaly detection systems, for example, IDES [12], flag observed activities that deviate significantly from the established normal usage profiles as anomalies, i.e., possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in his or her login sessions. If for a session that is being monitored, the frequencies are significantly

lower or higher, then an anomaly alarm will be raised. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may 'lot be able to describe what the attack is and may have high false positive rate.

Conceptually, an intrusion detection model, i.e., a misuse detection rule or a normal profile, has these two components:

- The *features* (or attributes, measures), e.g., "the number of failed login attempts", "the averaged frequency of the *9ce* command", etc., that together describe a logical event, e.g., a user login session;
- the *modeling algorithm,* e.g., rule-based pattern matching, that uses the features to - justify intrusions. Intrusion detection may find it increasingly difficult to distinguish false alarms from real intrusions.

Defining a set of *predicative* features that accurately capture the representative behaviors of intrusive or normal activities is the most important step in building an effective intrusion detection model and can be independent of the design of modeling algorithms.

PROBLEMS OF CURRENT IDS TECHNIQUES

The vast difference between the two networks makes it very difficult to apply intrusion detection techniques developed for a fixed wired network to an ad-hoc wireless network.

The most important difference is perhaps that the latter does not have a fixed infrastructure, and today's network based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. Compared with wired networks where traffic monitoring is usually done at switches, routers and gateways, an ad-hoc network does not have such traffic concentration points where the IDS can collect audit data for the entire network. Therefore, at anyone time, the only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms must be made to work on this partial and localized information.

In summary, we must answer the following research questions in developing a viable intrusion detection system for wireless ad-hoc networks:

What is a good system architecture for building intrusion detection and response systems that fits the features of \'\lireless ad-hoc networks ?

- What are the appropriate audit data sources? How do we detect anomaly based on partial, local audit traces - if they are the only reliable audit source?

What is a good model of activities in a wireless communication environment that can separate anomaly when under attacks from the normalcy?

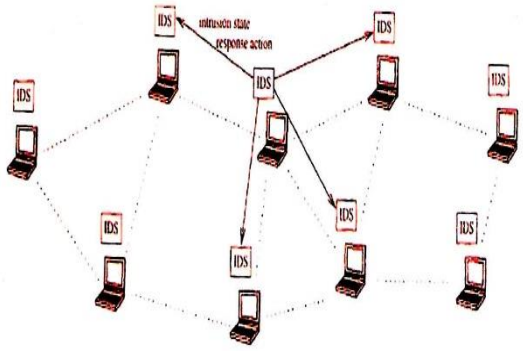

Fig-1: The IDS Architecture for Wireless Ad-Hoc Network

NETWORK INTRUSION DETECTION (IDS) IN MANET:

An intrusion detection system (IDS) collects and monitors operating system and network activity data, and analyses the information to determine whether there is an attack occurring. Current intrusion detection solutions rely on the relatively static and contained nature of wired networks. Potential intruders would need to gain physical access a network jack or logically enter the network through well-defined pathways. Placing detection sensors was a matter of finding (or creating) places where all these assumptions are no longer valid for wireless.

An ad network has some obvious disadvantages for intrusion detection [l]:

Wireless stations are all independent nodes. Each must be responsible for it's own protection from attack and compromise. Compromising only one node or introducing a malicious node may affect the viability of the entire network.

No point exists from which to monitor all network traffic.

Differences between normal and anomalous traffic patterns may be indistinguishable. The mobile nature of the wireless stations can make legitimate network traffic appear subject.

In [1] it is proposed an architecture where all nodes can act as independent IDS sensor; able to act independently and cooperatively. The possible intrusion events are generated from a local detection engine. If analysis of these events are inconclusive or require more information, local sensors can be utilized. Each independent sensor has six modules, three of which pertain to intrusion detection.

Data collection: the types of raw data the detection engines will utilize, include system and user activities, local communication activities, and "observable" (nodes within range) communications activities.

Local detection: since it will be difficult to maintain and distribute an anomalous signature database, [1] propose to define statistically "normal" activities specific to each node, which will therefore reside locally on each node.

Cooperative detection. If the local detection engine does not have enough evidence to alert on a suspected problem, it can ask other nodes for assistance. Information describing the event gets propagated to neighboring nodes. Evidence returned from neighboring nodes can be used to create a new evaluation of the event.

NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS)

Network intrusion detection system is intended to detect intrusion in the data passed through the network or sub-network to the attached users. NIDS listen to the network traffic passively and try to find out intrusions by comparing the audit data with the already known threats stored in its database. If at any stage a match happens, it generate alarm and notify the concerned administrator. The analysis session includes analysis of the packets, their payloads and IP address and ports. Such intrusion detection system is less expensive in terms of installation cost

as compared to HIDS. However, monitoring outgoing and incoming traffic of the whole network results in performance bottleneck. Moreover, they also cause communication delays. The NIDS suffers from issue of single point of failure.

HYBRID INTRUSION DETECTION SYSTEM

To overcome the above-mentioned drawbacks of HIDS and NIDS, another intrusion system namely Hybrid Intrusion Detection System is developed that combines features of both the IDSs. The hybrid IDS contain agents that play the role of communication between HIDS and NIDS. Mobile agents visit every host and perform detection process by checking log files of the system. Beside mobile agents, there are other agents, namely central agents that search the whole network to detect anomalies in traffic.

APPLICABILITY OF OTHER TECHNIQUES

Some other technique, like the flooding technique may also be adapted for use in an Ad Hoc network, essentially because its operation is based on the Gnutella protocol. In practice, however, it is unlikely that any benefit will be derived from doing so, since the technique essentially trades-off network reach with scalability. The low node count in Ad Hoc networks, however, implies that reducing network reach may significantly impact the probability of discovering the required content.

he hierarchical content discovery technique used in Fast Track, whilst achieving good scalability, introduces the concept of super node; one which is not easily adapted to an Ad Hoc network. Since all nodes in an Ad Hoc network generally make use of the same bandwidth, nodes with a higher bit rate connection cannot be identified. Secondly, within the super node layer, all super nodes can communicate directly with each other at these higher bit rates. Even if nodes with a higher bit rate connection are identified in an Ad Hoc network, these nodes wouldn't necessarily fall within radio range of each other. The Fast Track architecture may, however, prove useful in situations where gateways are provided to Ad Hoc networks. A gateway in this case could be designated as a super node and would have a fixed connection with the Internet. In this way, a technique such as that used in Fast Track can be extended to encompass Ad Hoc networks.

Content discovery as performed in Freenet is also unsuitable for Ad Hoc networks, since the advantages associated with this technique are not applicable to an Ad Hoc network.

Specifically, peers in Freenet are said to acquire a degree of specialisation in sourcing similar keys, as a result of route table entries added and content caching when a key travers the reverse path. This reverse path is not necessarily present in Ad Hoc networks.

On the other hand, the properties of CAN and Chord make them good candidates for use in Ad Hoc networks. Their low informational and communicational complexities are two such desirable properties. Having said this, an adaptation is definitely necessary in order to minimize or avoid the transfer of keys when peers join or leave the network. This is necessary due to the low bandwidth available to Ad Hoc nodes and due to the dynamic nature of Ad Hoc networks that is likely to make such transfers frequently necessary.

CONCLUSION

In this review, we briefly described ad hoc networks, their types and features. We also discussed the challenges faced by ad hoc networks, their security requirements and types of attacks encountered on various layers of ad hoc networks. We also elaborate the intrusion detection system, its working modules, challenges and its requirements in ad hoc networks. The paper categorized the IDS schemes based on various methodologies/techniques and explain the schemes developed for ad hoc networks, one by one. The working of each scheme, its strong points and limitations are clearly stated. Based on the study, we pointed out some of the open research issues and gave future research directions to help the researchers in the field of IDS in ad hoc networks.

REFERENCES

(1) X. Bangnan, S. Hischke, B. Walke, The role of ad hoc networking in future wireless communications, in: Proceedings of the International Conference on Communication Technology (ICCT), 2003.
(2) K. Yan, J. Tan, X. Fu, Improving energy efficiency of mobile devices by characterizing and exploring user behaviors, J. Syst. Arch. 98 (1) (2019) 126–134.
(3) Al Karaki, J. Nazzal, Infrastructureless wireless networks: cluster-based architectures and protocols, New Yark (2004)
(4) Oram A. PEER-TO-PEER - Harnessing the Power of Disruptive Technologies, California: O'Reilly & Associates, 2001. Perkins C. E. Ad Hoc Networking, New Jersey: Addison-Wesley, 2001.
(5) Stevens W. R. TCP/IP Illustrated, Volume 1 - The Protocols, Massachusetts: Addison - Wesley, 1994.
(6) R. Schollmeier, 1. Gruber, and M. Finkenzeller, "Routing in Mobile Ad Hoc a Peer-to-Peer Networks. A Comparison," in International Workshop on Peer-tc Computing, 2002, pp. 1-15.
(7) G. Kortuem, "When Peer-to-Peer comes Face-to-Face: Collaborative Peer-to Computing in Mobile Ad Hoc Networks," in First IEEE International Conference on Peer-to-Peer Computing, 2001, pp. 75-91.
(8) D. Doval and D. O'Mahoney, "Nom: Resource Location and Discovery for A Hoc Mobile Networks," in Proceedings of the First Annual Mediterranean Ac Hoc Networking Workshop, 2002, pp. 1-8.
(9) "Dictionary.com," [online] 2003, http://www.dictionary.com (Accessed: 25 August 2003).
(10) "ETSI HIPERLANIl Standard," (ETSI Telecom Standards), [online] 2003, http://portal.etsi.org/bran/ktalHiperlan/hiperlan 1.asp (Accessed: 16 August 21
(11) M. S. Gast, 802.11 Wireless Networks - The Definitive Guide, California: C & Associates, 2002.
(12) "Overview," (IEEE Standards Association), [online] 2003, http://standards.ieee.org/wireless/overview.htm1(Accessed: 16 August 2003).
(13) "ETSI HIPERLANI2 Standard," (ETSI Telecom Standards), [online] 003, http://porta1.etsi.orglbran/ktalhiperlan/hiperlan 2.asp (Accessed: 16 August 2003
(14) R. Schollmeier, "A Definition of Peer-to-Peer Networking for the C1assification of Peer- to-Peer Architectures and Applications," in First IEEE International Conference on Peer-to-Peer Computing, 2001, pp. 101-102.
(15) B. Leuf, Peer to Peer Collaboration and Sharing over the Internet, Indianapolin: Addison-Wesley, 2002.
(16) Kumar, S. (2020). Relevance of Buddhist Philosophy in Modern Management Theory. Psychology and Education, Vol. 58, no.2, pp. 2104–2111.
(17) Allugunti V.R (2022). A machine learning model for skin disease classification using convolution neural network. International Journal of Computing, Programming and Database Management 3(1), 141-147
(18) D. Barkai, "Technologies for Sharing and Collaborating on the Net," in First IEEE International Conference on Peer-to-Peer Computing, 2001, pp. 13-28.
(19) S. Keshav, An Engineering Approach to Computer Networking - ATM Network the Internet, and the Telephone Network, New Jersey: Addison-Wesley, 1997
(20) "TCPIIP," (Funet Network), [online] 2003, http://www.funet.fi/index/FUNET!history/internet/en/tcpip.htm1(Accessed: 17 August 2003).
(21) E. Thelen, "THE SRI VAN AND COMPUTER INTERNETWORKING," (Ed Thelen's Nike Missile Website), [online] 2003, http://ed-the1en.org/comp-hist/CORE-3-1-SRI-TCP-IP.htm1 (Accessed: 17 August 2003).
(22) D. Kristu1a, "The History of the Internet," (Dave's Site), [online] 2001, http://www.davesite.com/webstation/net-history.shtm1 (Accessed: 17 August, 2003).
(23) H. Wang, "Overview of Bluetooth Technology," Dept.of E1ectrica1 Engineering Penn State University Paper, pp. 1-42,2001.
(24) "Bluetooth," [online] 2003, https://www.bluetooth.org (Accessed: 22 August 2003).
(25) Anon., "IEEE 802.11 Technical Tutorial," Alvarion White Paper, pp. 1-17.