CHAPTER 2

INTRUSION DETECTION IN MOBILE AD HOC NETWORKS: RELATED WORK

2.1 INTRODUCTION

Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in MANET, any node may compromise the routing protocol functionality by disrupting the route discovery process.

2.2 LITERATURE SURVEY

2.2.1 Dynamically Self-organizing and Temporary Network Topologies

Hubaux et al. (2001) in an attempt, researched on mobile ad hoc networks has been focused primarily on routing issues. Security, on the other hand, has been given a lower priority. This work provides an overview of security problems for mobile ad hoc networks, distinguishing the threats on basic mechanisms and on security mechanisms. It then describes our solution to protect the security mechanisms. The original features of this solution
include that (i) it is fully decentralized and (ii) all nodes are assigned equivalent roles.

Boukerche (2001) proposed a mobile ad-hoc network (Manet) is a system of wireless mobile nodes dynamically self-organizing in arbitrary and temporary network topologies. People and vehicles can thus be internet worked in areas without a pre-existing communication infrastructure, or when the use of such infrastructure requires wireless extension. Therefore, such networks are designed to operate in widely varying environments, from military networks to low-power sensor networks and other embedded systems. Frequent topology changes caused by node mobility make routing in ad hoc wireless networks a challenging problem. We focus upon routing protocols for ad hoc networks. We study and compare the performance of several routing protocols. A variety of workload and scenarios using a variety of mobility, load and size of the ad hoc network were simulated.

In another proposal, Stajano & Anderson (1999) Imagine the future: hundreds of embedded computers per person, all cooperating via ad hoc wireless networks. What will the security implications be? Peer-to-peer and ubiquitous computing systems involve many principals, but their network connectivity is intermittent and not guaranteed. Traditional approaches to authentication, from Kerberos to public-key certificates, are therefore unworkable, because they rely on online connectivity to an authentication or revocation server. The work considers new solutions. It discusses the Resurrecting Duckling security policy model. The traditional taxonomy of security threats identifies three main classes which are considered: confidentiality, integrity or availability.

Unlike other authors, Vinayakray & Jani (2002), with the advancement in radio technologies like Bluetooth, IEEE 802.11 or Hiperlan, a new concept of networking has emerged. This is known as ad hoc networking
where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within ad hoc are mobile and they communicate with each other within radio range through direct wireless links or multihop routing.

Subsequently, Wrona (2002) analyzed security is a factor of an increasing importance in the design of modern communications systems. This is especially true for decentralized communications systems like wireless ad hoc networks. The work discusses security requirements for wireless ad hoc networks and gives an overview of related research projects.

Fugetto et al. (1998) in an attempt, the technologies, architectures, and methodologies traditionally used to develop distributed applications exhibit a variety of limitations and drawbacks when applied to large scale distributed settings (e.g., the Internet). In particular, they fail in providing the desired degree of configurability, scalability, and customizability. To address these issues, researchers are investigating a variety of innovative approaches. The most promising and intriguing ones are those based on the ability of moving code across the nodes of a network, exploiting the notion of mobile code. As an emerging research field, code mobility is generating a growing body of scientific literature and industrial developments. Nevertheless, the field is still characterized by the lack of a sound and comprehensive body of concepts and terms.

Michiardi & Molva (2002) however used little information about the effects of security exposures in terms of network performance has previously been available. This work provides a simulation study that identifies security issues that are specific to MANET and that illustrate the effects of those threats on network performance when the DSR routing protocol is used. We focused our attention on the evaluation of network performance in terms of global throughput and delay of a mobile ad hoc
network where a defined percentage of nodes behaved selfishly. The simulation study brought up two important conclusions. First, it shows that security issues have to be taken into account at the early stages of a routing protocol design. Indeed, when no countermeasures are taken, the simulation results showed that network operation and maintenance can be easily jeopardized and network performance will severely degrade. Second, a cooperative security scheme seems to be a reasonable solution to the selfishness problem: a selfish behavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not misbehave.

Harrison et al. (1995) proposed Mobile agents programs, typically written in a script language, which may be dispatched from a client computer and transported to a remote server computer for execution. Several authors have suggested that mobile agents offer an important new method of performing transactions and information retrieval in networks. Other writers have pointed out, however, that mobile agent introduce severe concerns for security. We consider the advantages offered by mobile agents and assess them against alternate methods of achieving the same function. We conclude that, while the individual advantages of agents do not represent an overwhelming motivation for their adoption, the creation of a pervasive agent framework facilitates a very large number of network services and applications.

Park et al. (1998) in another proposal deployed to expand the field of wireless products, the provision of authentication and privacy of the information transfer will be mandatory. These functions need to take into account the inherent limitations of the WLAN medium such as limited bandwidth, noisy wireless channel and limited computational power. Moreover, some of the IEEE 802.11 WLAN characteristics such as the use of
a point coordinator and the polling based Point Coordination Function (PCF) have also to be considered in this design. In this work, we introduce a security protocol for the IEEE 802.11 PCF that provides privacy and authentication, and is designed to reduce security overheads while taking into account the WLAN characteristics. We prove this protocol using the original and modified BAN logic.

Stajano (2002) discussed ubiquitous computing, over a decade in the making, has finally graduated from whacky buzzword through fashionable research topic to something that is definitely and inevitably happening. This will mean revolutionary changes in the way computing affects our society: changes of the same magnitude and scope as those brought about by the World Wide Web. When throw-away computing capabilities are embedded in shoes, drink cans and postage stamps, security and privacy take on entirely new meanings. Programmers, engineers and system designers will have to learn to think in new ways. Ubiquitous computing is not just a wireless version of the Internet with a thousand times more computers, and it would be a naive mistake to imagine that the traditional security solutions for distributed systems will scale to the new scenario.

Subsequently, Lee & Fan (2001) discuss Intrusion detection is an essential component of computer security mechanisms. It requires accurate and efficient analysis of a large amount of system and network audit data. It can thus be an application area of data mining. There are several characteristics of audit data: abundant raw data, rich system and network semantics, and ever "streaming". Accordingly, when developing data mining approaches, we need to focus on: feature extraction and construction, customization of (general) algorithms according to semantic information, and optimization of execution efficiency of the output models. In this work, we describe a data mining framework for mining audit data for intrusion
detection models. We discuss its advantages and limitations, and outline the open research problems.

Dokasetal (2002) in his work gives an overview of our research in building rare class prediction models for identifying known intrusions and their variations and anomaly/outlier detection schemes for detecting novel attacks whose nature is unknown. Experimental results on the KDDCup’99 data set have demonstrated that our rare class predictive models are much more efficient in the detection of intrusive behavior than standard classification techniques. Experimental results on the DARPA 1998 data set, as well as on live network traffic at the University of Minnesota, show that the new techniques show great promise in detecting novel intrusions. In particular, during the past few months our techniques have been successful in automatically identifying several novel intrusions that could not be detected using state-of-the-art tools such as SNORT. In fact, many of these have been on the CERT/CC list of recent advisories and incident notes.

Warrenderetal (1999) says intrusion detection systems rely on a wide variety of observable data to distinguish between legitimate and illegitimate activities. We study one such observable-sequences of system calls into the kernel of an operating system. Using system-call data sets generated by several different programs, we compare the ability of different data modeling methods to represent normal behavior accurately and to recognize intrusions. We compare the following methods: simple enumeration of observed sequences; comparison of relative frequencies of different sequences; a rule induction technique; and hidden Markov models (HMMs). We discuss the factors affecting the performance of each method and conclude that for this particular problem, weaker methods than HMMs are likely sufficient.
2.2.2 Pattern matching Intrusion Detection

Unlike other authors, Kumar & Spafford (1995) propose a Misuse Intrusion Detection has traditionally been understood in the literature as the detection of specific, precisely representable techniques of computer system abuse. Pattern matching is well disposed to the representation and detection of such abuse. Each specific method of abuse can be represented as a pattern and many of these can be matched simultaneously against the audit logs generated by the as kernel. Using relatively high level patterns to specify computer.

In another proposal, Eskin (2000) used Intrusion detection systems (IDSs) to maximize the realization of security goals while minimizing costs. In this work, we study the problem of building cost-sensitive intrusion detection models. We examine the major cost factors associated with an IDS, which include development cost, operational cost, damage cost due to successful intrusions, and the cost of manual and automated response to intrusions. These cost factors can be qualified according to a defined attack taxonomy and site-specific security policies and priorities. We define cost models to formulate the total expected cost of an IDS. We present cost-sensitive machine learning techniques that can produce detection models that are optimized for user-defined cost metrics. Empirical experiments show that our cost-sensitive modeling and deployment techniques are effective in reducing the overall cost of intrusion detection.

Ilgun (1995) in his work presents a new approach to representing and detecting computer penetrations in real time. The approach, called state transition analysis, models penetrations as a series of state changes that lead from an initial secure state to a target compromised state. State transition diagrams, the graphical representation of penetrations, identify precisely the requirements for and the compromise of a penetration and present only the critical events that must occur for the successful completion of the
penetration. State transition diagrams are written to correspond to the states of an actual computer system, and these diagrams form the basis of a rule based expert system for detecting penetrations, called the state transition analysis tool (STAT). The design and implementation of a Unix specific prototype of this expert system, called USTAT, is also presented.

Lee & Stolfo (2000) presents Intrusion detection is an important component of infrastructure protection mechanisms. Intrusion detection systems (IDSs) need to be accurate, adaptive, and extensible. Given these requirements and the complexities of today's network environments, we need a more systematic and automated IDS development process rather than the pure knowledge encoding and engineering approaches. This article describes a novel framework, MADAM ID, for Mining Audit Data for Automated Models for Intrusion Detection. This framework uses data mining algorithms to compute activity patterns from system audit data and extracts predictive features from the patterns. It then applies machine learning algorithms to the audit records that are processed according to the feature definitions to generate intrusion detection rules.

In another proposal Zhangetal (2003) proposed the rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. We need to search for new architecture and mechanisms to protect the wireless networks and mobile computing application. In this work, we examine the vulnerabilities of wireless networks and argue that we must include intrusion detection in the security architecture for mobile computing environment. We have developed such an architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc network, through simulation experiments.
Similarly, Satyanarayanan et al (1993) in his work present qualitative and quantitative data on file access in a mobile computing environment. This information is based on actual usage experience with the Coda File System over a period of about two years. Our experience confirms the viability and effectiveness of disconnected operation. It also exposes certain deficiencies of the current implementation of Coda, and identifies new functionality that would enhance its usefulness for mobile computing. The work concludes with a description of what we are doing to address these issues.

Heady et al (1990) presented the preliminary architecture of a network level intrusion detection system. The proposed system will monitor base level information in network packets (source, destination, packet size, and time), learning the normal patterns and announcing anomalies as they occur. The goal of this research is to determine the applicability of current intrusion detection technology to the detection of network level intrusions. In particular, we are investigating the possibility of using this technology to detect and react to worm programs.

Kachirski & Guha (2002) in their work proposed a distributed intrusion detection system for ad hoc wireless networks based on mobile agent technology. Wireless networks are particularly vulnerable to intrusion, as they operate in open medium, and use cooperative strategies for network communications. By efficiently merging audit data from multiple network sensors, we analyze the entire ad hoc wireless network for intrusions and try to inhibit intrusion attempts. In contrast to many intrusion detection systems designed for wired networks, we implement an efficient and bandwidth-conscious framework that targets intrusion at multiple levels and takes into account the distributed nature of ad hoc wireless network management and decision policies.
A model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer abuse is described. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system.

### 2.2.3 Intrusion Detection System in Distributed Systems

In another proposal, Sander & Tschudin (1998) devised Mobile code technology has become a driving force for recent advances in distributed systems. The concept of the mobility of executable code raises major security problems. In this work, we deal with the protection of mobile code from possibly malicious hosts. We conceptualize the specific cryptographic problems posed by mobile code, and we are able to provide a solution for some of these problems. We present techniques to achieve “non-interactive evaluation with encrypted functions” in certain cases and give a complete solution for this problem in important instances. We further present a way in which an agent might securely perform a cryptographic primitive-digital signing-in an untrusted execution environment. Our results are based on the use of homomorphic encryption schemes and function composition techniques.

Brutch & Brutch (1998) used distributed networked environment, security systems for network access and communication are necessary to allow legitimate hosts on the network to access the network services while
denying non-registered hosts. Ideally, such systems should ensure both confidentiality and integrity of messages exchanged over the network. We discuss the deficiencies with the registration and authentication services provided by Global System for Mobile Communication (GSM), Cellular Digital Packet Data (CDPD), and IS-41. Next, we present the design of the Mutual Authentication, Confidentiality, and Key MANagement (MACKMAN) system to provide a more secure registration and authentication service for mobile computing and wireless communication. The capabilities provided by MACKMAN include registration of legitimate hosts with the network, mutual authentication, and data confidentiality and integrity in a mobile and wireless environment. Data confidentiality and integrity are provided by using the public key Elliptic Curve RSA (ECRSA) cryptosystem in conjunction with a hierarchy of certification authorities for key distribution and management.

Subsequently, Bhargava et al. (2000) presents Survivability and secure communications are essential in a mobile computing environment. In a secure network, all the hosts must be authenticated before communicating, and failure of the agents that authenticate the hosts may completely detach the hosts from the rest of the network. In this work, we describe two techniques to eliminate such a single point of failure. Both of these approaches make use of backup servers, but they differ in the way they are organized and deployed. We evaluate our proposed architectures with a prototype system that we built. We also identify various security threats and performance issues in group (multicast) communications in mobile computing environments. We propose a scheme for efficient key distribution and management using key graphs to provide secure multicast service.

Again, Jansen & Karygiannis (1999) propose a Mobile agent technology offers a new computing paradigm in which a program, in the form
of a software agent, can suspend its execution on a host computer, transfer itself to another agent-enabled host on the network, and resume execution on the new host. The use of mobile code has a long history dating back to the use of remote job entry systems in the 1960's. Today's agent incarnations can be characterized in a number of ways ranging from simple distributed objects to highly organized software with embedded intelligence. As the sophistication of mobile software has increased over time, so too have the associated threats to security. This report provides an overview of the range of threats facing the designers of agent platforms and the developers of agent-based applications. The report also identifies generic security objectives, and a range of measure for countering the identified threats and fulfilling these security objectives.

As a consequence, Fugettoetal (1998) used the technologies, architectures, and methodologies traditionally used to develop distributed applications exhibit a variety of limitations and drawbacks when applied to large scale distributed settings (e.g., the Internet). In particular, they fail in providing the desired degree of configurability, scalability, and customizability. To address these issues, researchers are investigating a variety of innovative approaches. The most promising and intriguing ones are those based on the ability of moving code across the nodes of a network, exploiting the notion of mobile code. As an emerging research field, code mobility is generating a growing body of scientific literature and industrial developments. Nevertheless, the field is still characterized by the lack of a sound and comprehensive body of concepts and terms. As a consequence, it is rather difficult to understand, assess, and compare the existing approaches. In turn, this limits our ability to fully exploit them in practice, and to further promote the research work on mobile code.

Johansen et al (1995) investigating networking agents for its use in large scale distributed computing. This is organized in the TACOMA
(Tromsø And COrnell Moving Agents) project. This chapter presents the background of and the framework for the TACOMA project.

Askwith et al (1997) proposed a Third generation mobile networks aim to offer `any service, anywhere, at any time'. Users require privacy within these systems in order to feel confident of their use. Privacy requirements (in mobile networks) are: content, location and identification privacy, and authentication. Differing from previous approaches to privacy, the network itself is considered to be an untrusted party. The work proposes a scheme that allows the user to register with the network and remain anonymous (both location and identification). Digital mixes are used to create anonymity and authentication is achieved through a token based scheme. Finally the aspect of information leaking to authorised third parties is discussed and billing requirements are detailed which involve the use of `coin' like tokens traded for services.

Similarly, Vemulapalli et al (2002) proposed security for digital libraries is challenging due to their dynamic and distributed nature. The need for security for digital libraries arises from legal, social and sensitivity issues of information. Increased dependence on agent-based architectures for digital libraries and peer-to-peer communications makes them more vulnerable to security threats. Thus, evolving a comprehensively secure distributed digital library system is challenging. In addition to the security guarantees, performance guarantees such as convenience in usage, minimal response time, and high throughput are also required of these systems. In this work, we address the issues of integrating performance and security in digital libraries. We discuss a variety of security tools that are currently available and their impact on security and performance of digital library systems.

Ferrari et al (2002) in an attempt introduce several challenging requirements with respect to the formulation, specification, and enforcement
of adequate data protection policies. Unlike conventional database environments, a DL environment typically is characterized by a dynamic subject population, often making accesses from remote locations, and by an extraordinarily large amount of multimedia information, stored in a variety of formats. Moreover, in a DL environment, access policies are often specified based on subject qualifications and characteristics, rather than subject identity. Traditional authorization models are not adequate to meet access control requirements of DLs. In this work, we present a Digital Library Authorization System (DLAS).

2.2.4 Autonomous Self-organizing System

Awerbuch et al (2002) uses an ad hoc wireless network is an autonomous self-organizing system of mobile nodes connected by wireless links where nodes not in direct range can communicate via intermediate nodes. A common technique used in routing protocols for ad hoc wireless networks is to establish their routing paths on-demand, as opposed to continually maintaining a complete routing table. A significant concern in routing is the ability to function in the presence of byzantine failures which include nodes that drop, modify, or mis-route packets in an attempt to disrupt the routing service. We propose an on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes. Our adaptive probing technique detects a malicious link after \( \log n \) faults have occurred, where \( n \) is the length of the path. These links are then avoided by multiplicatively increasing their weights and by using an on-demand route discovery protocol that finds a least weight path to the destination.

Papadimitratos & Haas (2002) discussed the emergence of the Mobile Ad Hoc Networking (MANET) technology advocates self-organized wireless interconnection of communication devices that would either extend
or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the proliferation of MANET-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met.

In another work, presents a route discovery protocol that mitigates the detrimental effects of such malicious behavior, as to provide correct connectivity information. Our protocol guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying node. Furthermore, the protocol responsiveness is safeguarded under different types of attacks that exploit the routing protocol itself. The sole requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. Specifically, no assumption is made regarding the intermediate nodes, which may exhibit arbitrary and malicious behavior. The scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner.

Additionally, Michiardi & Molva(2002) Countermeasures against denial of service attacks and node misbehaviour are mandatory requirements in MANET. Essential network operations assuring basic connectivity can be heavily jeopardized by nodes that do not properly execute their share of the network operations. We suggest a security mechanism based on a collaborative monitoring technique that prevents active and passive denial of service attacks by enforcing node cooperation. This mechanism can be smoothly extended to basic network functions with little impact on existing protocols. We also investigate on some attacks scenarios in order to analyze the robustness of the proposed security scheme.
Buchegger & Boudec (2002) Devices a mobile ad hoc networks work as network nodes and relay packets originated by other nodes. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. For individual nodes it might be advantageous not to cooperate. The new routing protocol extensions presented in this work make it possible to detect and isolate misbehaving nodes, thus making denying cooperation undesirable. In the presented scheme, trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes. A hybrid scheme of selective altruism and utilitarianism is presented to strengthen mobile ad hoc network protocols in their resistance to security attacks, while aiming at keeping network throughput high. This work focuses particularly on the network layer using the dynamic source routing (DSR) protocol as an example.

Subsequently, Buttyán & Hubaux (2003), used military and rescue applications of mobile ad hoc networks, all the nodes belong to the same authority; therefore, they are motivated to cooperate in order to support the basic functions of the network. In this work, we consider the case when each node is its own authority and tries to maximize the benefits it gets from the network. More precisely, we assume that the nodes are not willing to forward packets for the benefit of other nodes. This problem may arise in civilian applications of mobile ad hoc networks. In order to stimulate the nodes for packet forwarding, we propose a simple mechanism based on a counter in each node. We study the behavior of the proposed mechanism analytically and by means of simulations, and detail the way in which it could be protected against misuse.

In contrast with conventional networks, mobile ad hoc networks usually do not provide online access to trusted authorities or to centralized servers, and they exhibit frequent partitioning due to link and node failures.
and to node mobility. For these reasons, traditional security solutions that require online trusted authorities or certificate repositories are not well-suited for securing ad hoc networks. We propose a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, our approach does not require any trusted authority, not even in the system initialization phase.

Unlike other authors, Yi & Kravets (2002) recognized as one of the most effective mechanisms for providing fundamental security services including authentication, digital signatures and encryption for dynamic networks. Effective management of keys, or digital certificates holding the keys, is one of the key factors for the successful wide-spread deployment of public key cryptography. The public key infrastructure (PKI), an infrastructure for managing digital certificates, was introduced for this purpose. The most important component of PKI is the certificate authority (CA), the trusted entity in the system that vouches for the validity of digital certificates. This work describes a framework to provide efficient yet effective distributed CA service for ad hoc wireless networks. We select physically or computationally more secure nodes as MOCAs (MOBILE Certificate Authority) and use threshold cryptography to distribute the CA's private key among these MOCA nodes. We also provide a protocol for clients to contact MOCAs and get certification services without incurring excessive overhead.

Countermeasures for node misbehavior and selfishness are mandatory requirements in MANET. Selfishness that causes lack of node activity cannot be solved by classical security means that aim at verifying the correctness and integrity of an operation. We suggest a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET to
prevent selfish behavior. Each network entity keeps track of other entities’
collaboration using a technique called reputation. The reputation is calculated
based on various types of information on each entity’s rate of collaboration.
Since there is no incentive for a node to maliciously spread negative
information about other nodes, simple denial of service attacks using the
collaboration technique itself are prevented. The generic mechanism can be
smoothly extended to basic network functions with little impact on existing
protocols.

Again, Avoine & Vaudenay (2003) in contrast with traditional
cryptographic protocols in which parties can have access to common third
parties, and where at least one of them is assumed to be honest, we propose
here a new model which is relevant for networks of communication devices
with security modules. We then focus on the problem of fair exchange in this
model. We propose a probabilistic protocol which provides arbitrarily low
unfairness (involving a complexity cost).

In another proposal, Ramanujam et al (2000) in his work presents a
set of design techniques, collectively called TIARA (Techniques for
Intrusion-resistant Ad Hoc Routing Algorithms), to protect ad hoc networks
against denial of service attacks. The TIARA mechanisms described seek to
limit the damage sustained by ad hoc networks from intrusion attacks and
allow for continued network operation at an acceptable level during such
attacks. These mechanisms are designed to handle attacks on the routing
traffic as well as the data traffic in ad hoc networks thereby providing a
comprehensive defense against intruders. TIARA is routing algorithm
independent. That is, TIARA may be viewed as providing general design
principles and techniques the can be incorporated within a number of existing
ad hoc routing algorithms to make them robust to intrusion attacks.
In an attempt, Hu et al (2002) used an ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this work, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

2.2.5 Authenticated Link-level Ad hoc Routing Protocol

Brinkley & Trost (2001) designed an authenticated link-level ad hoc routing protocol and integrated it with the Portland State University implementation of Mobile-IP. The routing protocol addresses link security issues. In our protocol, mobile nodes, as well as agents, broadcast ICMP router discovery packets. The router discovery packets are authenticated and bind the sender's MAC and IP addresses. Problems caused by tying IP subnet schemes to routing on radio links are eliminated. Security problems associated with ARP spoofing are also reduced. This link-level protocol is integrated with Mobile-IP on links where increased security is needed. The
protocol replaces ARP, and may be integrated with higher-level multi-hop ad hoc routing protocols.

Yang et al (2002) describes unified network-layer security solution in ad hoc networks, which protects both routing and packet forwarding functionalities in the context of the AODV protocol. To address the unique characteristics of ad hoc networks, we take a self-organized approach by exploiting full localized design, without assuming any a priori trust or secret association between nodes. In our design, each node has a token in order to participate in the network operations, and its local neighbors collaboratively monitor it to detect any misbehavior in routing or packet forwarding services. Upon expiration of the token, each node renews its token via its multiple neighbors. The period of the validity of a node's token is dependent on how long it has stayed and behaved well in the network. A well-behaving node accumulates its credit and renews its token less and less frequently as time evolves. In essence, our security solution exploits collaboration among local nodes to protect the network layer without completely trusting any individual node.

Luo & Lu (2000) in their work Providing security support for large ad hoc wireless networks is challenging due to their unique characteristics, such as mobility, channel errors, dynamic node joins and leaves, and occasional node break-ins. In this report, we exploit these characteristics and present our design that supports ubiquitous security for mobile nodes, scales to network size, and is robust against adversary break-ins. In our design, we distribute the functionality of conventional security servers, specifically the authentication services, so that each individual node can potentially provide other services.

Hu et al (2002) presents an ad hoc network is a group of wireless mobile computers (or nodes), in which individual nodes cooperate by
forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting assuming a trusted environment. In this work, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, is efficient, using only highly efficient symmetric cryptographic primitives.

Yi et al (2001) proposes a new routing technique called Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. We develop a two-tier classification of routing protocol security metrics, and propose a framework to measure and enforce security attributes on ad hoc routing paths. Our framework enables applications to adapt their behavior according to the level of protection available on communicating nodes in an ad hoc network.

Marti et al (2000) in his work describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can
increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

Zhou & Haas (1999) presents Ad hoc networks in a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in the design of these networks is their vulnerability to security attacks. In this article, we study the threats on ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks - multiple routes between nodes - to defend routing against denial-of-service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which terms the core of our security framework.

Mobile ad hoc networks are infrastructure-free, pervasive, ubiquitous and without any centralized authority. These unique characteristics, combined with security threats, demand solutions for securing ad hoc networks prior to their deployment in commercial and military applications. So far, the research in mobile ad hoc network has been primarily focused on routing and mobility aspects rather than securing the ad hoc network itself. Due to the ever-increasing security threats, there is a need to develop algorithms and protocols for a secured ad hoc network infrastructure. This work surveys the prevailing mobile ad hoc network security threats and the existing solution schemes.
Similarly, Kongetal (2002) discusses a secure communication is critical in military environments in which the network infrastructure is vulnerable to various attacks and compromises. A conventional centralized solution breaks down when the security servers are destroyed by the enemies. In this work, we design and evaluate a security framework for multilevel ad hoc wireless networks with unmanned aerial vehicles (UAVs). In battlefields, the framework adapts to the contingent damages on the network infrastructure.

Depending on the availability of the network infrastructure, our design is composed of two modes. In infrastructure mode, security services, specifically the authentication services, are implemented on UAVs that feature low overhead and flexible managements. When the UAVs fail or are destroyed, our system seamlessly switches to infrastructureless mode, a backup mechanism that maintains comparable security services among the surviving units. In the infrastructureless mode, the security services are localized to each node's vicinity to comply with the ad hoc communication mechanism in the scenario. We study the instantiation of these two modes and the transitions between them. Our implementation and simulation measurements confirm the effectiveness of our design.

Sun et al (2006) addresses the main challenges in building intrusion detection systems (IDSs) for mobile ad hoc networks (MANETs) is to integrate mobility impacts and to adjust the behaviour of IDSs correspondingly. In this work, we first introduce two different approaches, a Markov chain-based approach and a Hotelling's T2 test based approach, to construct local IDSs for MANETs. We then demonstrate that nodes' moving speed, a commonly used parameter in tuning IDS performances, is not an effective metric to tune IDS performances under different mobility models. To solve this problem, we further propose an adaptive scheme, in which
suitable normal profiles and corresponding proper thresholds can be
selected adaptively by each local IDS through periodically measuring its
local link change rate, a proposed unified performance metric. We study the
proposed adaptive mechanism at different mobility levels, using different
mobility models such as random waypoint model, random drunken model,
and obstacle mobility model. Simulation results show that our proposed
adaptive scheme is less dependent on the underlying mobility models and can
further reduce false positive ratio.

2.2.6 Mobile Agents based IDS

Flexible and distributed management systems based on mobile
agents have certain advantages over centralized and static management
architectures. However, security plays a decisive role in terms of acceptance
and applicability of mobile agents. In this work we analyze the threats and
attacks against mobile agent systems used for management purposes.
Therefore, general models of mobile agent based management systems are
developed. Based on a risk analysis of these models we derive security
requirements. In order to satisfy these requirements components and services
are identified and integrated in a comprehensive security architecture

In another proposal Farmer et al (1996) processes Mobile agents
are which can autonomously migrate to new hosts. Despite its many practical
benefits, mobile agent technology results in significant new security threats
from malicious agents and hosts. The primary added complication is that, as
an agent traverses multiple hosts that are trusted to different degrees, its state
can change in ways that adversely impact its functionality. In this work, we
investigatethese new threats and develop a set of achievable security
requirements for mobile agent systems.
Blaek (1998) uses a mobile agent is an autonomous computer program which can migrate from machine to heterogeneous machine. An agent server which receives a mobile agent can easily make a copy of the mobile agent, because a mobile agent is just a program consisting of code and data. We define a mobile agent clone as the copied agent. It is impossible to distinguish between a mobile agent clone and its original agent. This causes problems connected with agent authentication, unexpected multiple transactions, and other security issues. In this work, we investigate the problems caused by mobile agent clones and we design a protocol, which detects agent clone executions and identifies the clone generating agent server. Finally, we prove the correctness of the protocol formally, through Coloured Petri Nets.

Kachirski & Guha (2003) in his work propose a distributed intrusion detection system for ad hoc wireless networks based on mobile agent technology. Wireless networks are particularly vulnerable to intrusion, as they operate in open medium, and use cooperative strategies for network communications. By efficiently merging audit data from multiple network sensors, we analyze the entire ad hoc wireless network for intrusions and try to inhibit intrusion attempts. In contrast to many intrusion detection systems designed for wired networks, we implement an efficient and bandwidth-conscious framework that targets intrusion at multiple levels and takes into account distributed nature of ad hoc wireless network management and decision policies.

Huang & Lee (2003) presents a Mobile ad hoc networking (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. MANETs are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and
management point, and lack of a clear line of defense. In this work, we report our progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, we can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. We address the run-time resource constraint problem using a cluster-based detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness. We have conducted extensive experiments using the ns-2 and MobiEmu environments to validate our research.

Albers & Camp (2002) discuss the performances of wireless technologies have increased tremendously thus opening new fields of application in the domain of networking. One of such fields concerns mobile adhoc networks (MANETs) in which mobile nodes organise themselves in a network without the help of any predefined infrastructure. Securing MANETs is just as important, if not more, as securing traditional wired networks. Existing solutions can be used to obtain a certain level of security. Nevertheless, these solutions may not always be suitable to wireless networks. Furthermore, ad hoc networks have their own vulnerabilities that cannot be tackled by these solutions. To obtain an acceptable level of security in such a context, traditional security solutions should be coupled with an intrusion detection mechanism. In this work we show how ad hoc networks can be, to a certain extent, secured using traditional techniques. We then examine the different intrusion detection techniques and point out the reasons why they usually cannot be used in an ad hoc context. Finally, we go through the
requirements of an intrusion detection system for ad hoc networks, and define an adapted architecture for an intrusion detection system for manets.

Intrusion detection systems (IDSs) for mobile ad hoc networks (MANETs) are necessary when we deploy MANETs in reality. In this work, focusing on the protection of MANET routing protocols, we present a new intrusion detection agent model and utilize a Markov chain based anomaly detection algorithm to construct the local detection engine. The details of feature selection, data collection, data preprocess, Markov chain construction, classifier construction and parameter tuning are provided. Based on the routing disruption attack aimed at the dynamic source routing protocol (DSR), we study the performance of the algorithm at different mobility levels. Simulation results show that our algorithm can achieve low false positive ratio, high detection ratio, and small MTFA (mean time to the first alarm), especially when the mobility is low. Detailed analysis of simulation results is also presented.

Similarly, Huang et al (2003) presents the proliferation of wireless devices, mobile ad-hoc networking (MANET) has become a very exciting and important technology. However, MANET is more vulnerable than wired networking. Existing security mechanisms designed for wired networks have to be redesigned in this new environment. In this work, we discuss the problem of intrusion detection in MANET. The focus of our research is on techniques for automatically constructing anomaly detection models that are capable of detecting new (or unseen) attacks. We introduce a new data mining method that performs "cross-feature analysis" to capture the inter-feature correlation patterns in normal traffic. These patterns can be used as normal profiles to detect deviation (or anomalies) caused by attacks. We have implemented our method on a few well known ad-hoc routing protocols, namely, Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance
Vector (AODV), and have conducted extensive experiments on the ns-2 simulator. The results show that the anomaly detection models automatically computed using our data mining method can effectively detect anomalies caused by typical routing intrusions.

The Ad hoc On-Demand Distance Vector (AODV) routing protocol, designed for mobile ad hoc networks, offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization. However, without keeping in mind the security issues in the protocol design, AODV is vulnerable to various kinds of attacks. This work analyzes some of the vulnerabilities, specifically discussing attacks against AODV that manipulate the routing messages. We propose a solution based on specification-based intrusion detection to detect attacks on AODV. Briefly, our approach involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. In addition, one additional field in the protocol message is proposed to enable the monitoring. We illustrate that our algorithm, which employs a tree data structure, can effectively detect most of the serious attacks in real time and with minimum overhead.

Puttini et al (2003) In his work propose a distributed and modular architecture for an intrusion detection system (IDS) dedicated to a mobile ad hoc network (MANET) environment. The main feature of our proposition relies on the use, on each node of the MANET, of a local IDS (LIDS) cooperating with other LIDSes through the use of mobile agents. The modular design is needed as a response to the extensibility requirements related to the complex contexts of MANET. The proposed solution has been validated by a proof-of-concept prototype, which is described in the work. Two different types of attacks are presented and have been implemented, at the network
level and at the application level. The detection of such attacks are formally described by specification of data collection, attack signatures associated with such data and alerts generation, emphasizing the relation of each of these detection steps with the modules in the designed architecture. The use of the management information base (MIB) as a primary data source for the detection process is discussed and modules for MIB data extraction and processing are specified and implemented in the prototype. Experiments exhibit fairly good results, the attacks being collaboratively detected in real-time.

Brutch & Ko (2003) presents a brief survey of current research in intrusion detection for wireless ad-hoc networks. In addition to examining the challenges of providing intrusion detection in this environment, this work reviews current efforts to detect attacks against the ad-hoc routing infrastructure, as well as detecting attacks directed against the mobile nodes. This work also examines the intrusion detection architectures that may be deployed for different wireless ad-hoc network infrastructures, as well as proposed methods of intrusion response.

Subsequently, Mukherjee et al (1994) says Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current "open" mode. The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems (IDSs) are based on the beliefs that an intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized
actions are detectable. Typically, IDSs employ statistical anomaly and rule-based misuse models in order to detect intrusions. A number of prototype IDSs have been developed at several institutions, and some of them have also been deployed on an experimental basis in operational systems. In the present work, several host-based and network-based IDSs are surveyed, and the characteristics of the corresponding systems are identified. The host-based systems employ the host operating system's audit trails as the main source of input to detect intrusive activity, while most of the network-based IDSs build their detection mechanism on monitored network traffic, and some employ host audit trails as well. An outline of a statistical anomaly detection algorithm employed in a typical IDS is also included.

Janakiraman et al. (2003) discuss while the spread of the Internet has made the network ubiquitous, it has also rendered networked systems vulnerable to malicious attacks orchestrated from anywhere. These attacks or intrusions typically start with attackers infiltrating a network through a vulnerable host and then launching further attacks on the local network or Intranet. Attackers rely on increasingly sophisticated techniques like using distributed attack sources and obfuscating their network addresses. On the other hand, software that guards against them remains rooted in traditional centralized techniques, presenting an easily-targeted single point of failure. Scalable, distributed network intrusion prevention techniques are sorely needed. We propose Indra - a distributed scheme based on sharing information between trusted peers in a network to guard the network as a whole against intrusion attempts. We present initial ideas for running Indra over a peer-to-peer infrastructure to distribute up-to-date rumors, facts, and trust information in a scalable manner.

Unlike other authors, Debar & Wespi (2001) describes an aggregation and correlation algorithm used in the design and implementation
of an intrusion-detection console built on top of the Tivoli Enterprise Console (TEC). The aggregation and correlation algorithm aims at acquiring intrusion-detection alerts and relating them together to expose a more condensed view of the security issues raised by intrusion-detection systems.

Sekar (2002) Unlike signature or misuse based intrusion detection techniques, anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. This work presents a new approach that combines specification-based and anomaly-based intrusion detection, mitigating the weaknesses of the two approaches while magnifying their strengths. Our approach begins with state-machine specifications of network protocols, and augments these state machines with information about statistics that need to be maintained to detect anomalies. We present a specification language in which all of this information can be captured in a succinct manner. We demonstrate the effectiveness of the approach on the 1999 Lincoln Labs intrusion detection evaluation data, where we are able to detect all of the probing and denial-of-service attacks with a low rate of false alarms (less than 10 per day). Whereas feature selection was a crucial step that required a great deal of expertise and insight in the case of previous anomaly detection approaches, we show that the use of protocol specifications in our approach simplifies this problem. Moreover, the machine learning component of our approach is robust enough to operate without human supervision, and fast enough that no sampling techniques need to be employed. As further evidence of effectiveness, we present results of applying our approach to detect stealthy email viruses in an intranet environment.
2.2.7 Machine Learning for IDS

A time-based inductive learning approach to security audit trail analysis is presented. The approach uses a time-based inductive engine to generate rule-based sequential patterns that characterize the behavior of a user. The time-based inductive approach substantially increases the discriminating capability of an anomaly detection system due to the added dimension of information given in the sequential relationships between security events. It is shown that the use of rule-based sequential patterns allows a security auditing system to capture characteristics of user behavior that may be otherwise intractable using traditional statistical approaches. The approach also may help security management to focus on a few potentially hostile security events inside an entire user log-in session.

Haystack is a prototype system for the detection of intrusions in multiuser US Air Force computer systems. Haystack reduces voluminous system audit trails to short summaries of user behavior, anomalous events, and security incidents. This is designed to help the system security officer detect and investigate intrusions, particularly by insiders (authorized users). Haystack's operation is based on behavioral constraints imposed by security policies and on models of typical behavior for user groups and individual users.

Alampalayam & Kumar (2004) propose a practical and predictive security model for intrusion detection in a computer networking environment using data mining. This model uses a classification and regression technique for data mining. The goal of the proposed model is to identify significant variables that measure network intrusion from a wealth of raw network data and perform an efficient vulnerability evaluation based on those variables. Analysis of experimental results conducted using the DARPA benchmark dataset shows that the CART (classification and regression trees) approach
performs better compared to other models, like random projection and principal component analysis. The results also indicate that the performance of the CART approach in the proposed model is not significantly affected, even as the dimension of the input data decreases, without compromising the prediction success rate.

Again, Alampalayam & Kumar (2003) proposed an adaptive security scheme for denial of service security threats in mobile agent system based on wireless ad hoc network environment. This model is based on a fuzzy feedback controller and allows the ad hoc mobile network user to select the security level and requirement he/she needs. Our model integrates the existing security techniques in providing adaptive security for mobile agents in ad hoc network. The goal of the proposed scheme is to provide a security framework that will detect automatically various attacks and then take appropriate measures to deal with the attack. We have simulated the proposed scheme and conducted experiments for selected denial of service attacks.

Most existing reliability analyses provide a quantitative assessment of the overall system reliability assuming that the components of a system can operate only in two modes: completely operational or non-operational. We have developed an Extended Reliability Evaluation Framework (X-REF) to compute the system reliability in a quantitative form as well as in a qualitative form. In the extended framework, the components of a computer system can operate in any number of degraded modes of operation. The state of a component is given by a reliability profile which represents the component’s reliability values and their associated degree of certainty. The inputs needed for X-REF are component reliability profiles and the fault tree of the system. An effective technique is developed to combine these component reliability profiles using the fault tree as a configuration to represent system failure for computing the overall reliability profile of the system.
The problem of bias in split variable selection in classification tree construction. A split criterion is unbiased if the selection of a split variable $X$ is based only on the strength of the dependency between $X$ and the class label, regardless of other characteristics; otherwise the split criterion is biased. Our work makes the following four contributions: (1) we give a definition that allows us to quantify the extent of the bias of a split criterion, (2) we show that the p-value of any split criterion is a nearly unbiased criterion, (3) we give theoretical and experimental evidence that the correction is successful, and (4) we demonstrate the power of our method by correcting the bias of the gini gain.

Mobile ad hoc networks are infrastructure-free, pervasive and ubiquitous in nature, without any centralized authority. These unique characteristics coupled with the growing concerns for security attacks demand an immediate solution for securing the ad hoc network, prior to its full-fledged deployment in commercial and military applications. So far, most of the research in mobile ad hoc networks has been primarily focused on routing and mobility aspects rather than securing the ad hoc networks themselves. Due to ever increasing security threats, there is a need to develop schemes, algorithms, and protocols for a secured ad hoc network infrastructure. To realize this objective, we have proposed a practical and effective security model for mobile ad hoc networks. The proposed predictive security model is designed using a fuzzy feedback control approach. The model is based on identifying critical network parameters that are affected by various types of attacks and it continuously monitors those parameters. Once we measure the relative change in these parameter values, we could detect the type of attack accurately and protect the system, without compromising its effectiveness.

Viinikka & Debar (2004) presented an Intrusion detection systems typically create large amounts of alerts, processing of which is a time
consuming task for the user. This work describes an application of exponentially weighted moving average (EWMA) control charts used to help the operator in alert processing. Depending on his objectives, some alerts are individually insignificant, but when aggregated they can provide important information on the monitored system’s state. Thus it is not always the best solution to discard those alerts, for instance, by means of filtering, correlation, or by simply removing the signature. We deploy a widely used EWMA control chart for extracting trends and highlighting anomalies from alert information provided by sensors performing pattern matching. The aim is to make output of verbose signatures more tolerable for the operator and yet allow him to obtain the useful information available. The applied method is described and experimentation along its results with real world data are presented. A test metric is proposed to evaluate the results.

Pappasetal (2004) Overlay networks represent an emerging technology for rapid deployment of novel network services and applications. However, since public overlay networks are built out of loosely coupled end-hosts, individual nodes are less trustworthy than Internet routers in carrying out the data forwarding function. Here we describe a set of mechanisms designed to detect and repair errors in the data stream. Utilizing the highly redundant connectivity in overlay networks, our design splits each data stream to multiple sub-streams which are delivered over disjoint paths. Each sub-stream carries additional information that enables receivers to detect damaged or lost packets. Furthermore, each node can verify the validity of data by periodically exchanging Bloom filters, the digests of recently received packets, with other nodes in the overlay. We have evaluated our design through both simulations and experiments over a network testbed. The results show that most nodes can effectively detect corrupted data streams even in the presence of multiple tampering nodes.
Huang & Lee (2004) in an attempt analysis a challenging problem, especially in emerging environments where there are few known attack cases. One such new environment is the Mobile Ad hoc Network (MANET). In this work, we present a systematic approach to analyze attacks. We introduce the concept of basic events. An attack can be decomposed into certain combinations of basic events. We then define a taxonomy of anomalous basic events by analyzing the basic security goals.

Attack analysis provides a basis for designing detection models. We use both specification-based and statistical-based approaches. First, normal basic events of the protocol can be modeled by an extended finite state automaton (EFSA) according to the protocol specifications. The EFSA can detect anomalous basic events that are direct violations of the specifications. Statistical learning algorithms, with statistical features, i.e., statistics on the states and transitions of the EFSA, can train an effective detection model to detect those anomalous basic events that are temporal and statistical in nature.

We use the AODV routing protocol as a case study to validate our research. Our experiments on the MobiEmu wireless emulation platform show that our specification-based and statistical-based models cover most of the anomalous basic events in our taxonomy.

2.2.8 Routing Protocols for IDS

In another attempt Just et al (2003) presents most of the routing protocols in wireless ad hoc networks, such as DSR, assume nodes are trustworthy and cooperative. This assumption renders wireless ad hoc networks vulnerable to various types of Denial of Service (DoS) attacks. We present a distributed probing technique to detect and mitigate one type of DoS attacks, namely malicious packet dropping, in wireless ad hoc networks. A malicious node can promise to forward packets but in fact fails to do so. In
our distributed probing technique, every node in the network will probe the other nodes periodically to detect if any of them fail to perform the forwarding function. Subsequently, node state information can be utilized by the routing protocol to bypass those malicious nodes. Our experiments show that in a moderately changing network, the probing technique can detect most of the malicious nodes with a relatively low false positive rate. The packet delivery rate in the network can also be increased accordingly.

Consequently, Liu et al (2005) uses sensors' locations play a critical role in many sensor network applications. A number of techniques have been proposed recently to discover the locations of regular sensors based on a few special nodes called beacon nodes, which are assumed to know their locations (e.g., through GPS receivers or manual configuration). However, none of these techniques can work properly when there are malicious attacks, especially when some of the beacon nodes are compromised. This work introduces a suite of techniques to detect and remove compromised beacon nodes that supply misleading location information to the regular sensors, aiming at providing secure location discovery services in wireless sensor networks. These techniques start with a simple but effective method to detect malicious beacon signals. To identify malicious beacon nodes and avoid false detection, this work also presents several techniques to detect replayed beacon signals. This work then proposes a method to reason about the suspiciousness of each beacon node at the base station based on the detection results collected from beacon nodes, and then revoke malicious beacon nodes accordingly. Finally, this work provides detailed analysis and simulation to evaluate the proposed techniques. The results show that our techniques are practical and effective in detecting malicious beacon nodes.

Reputation systems help peers decide whom to trust before undertaking a transaction. Conventional approaches to reputation-based trust
modeling assume that peers reputed to provide trustworthy service are also likely to provide trustworthy feedback. By basing the credibility of a peer’s feedback on its reputation as a transactor, these models become vulnerable to malicious nodes that provide good service to badmouth targeted nodes. We propose to decouple a peer’s reputation as a service provider from its reputation as a service recommender, making the reputation more robust to malicious peers. We show via simulations that a decoupled approach greatly enhances the accuracy of reputations generated, resulting in fewer malicious transactions, false positives, and false negatives.

Additionally, Ocakoglu et al (2004) in his work, propose an attack model against DSR ad hoc network routing protocol and analyze the effects of this attack model on DSR route discovery mechanism. The analysis of the attack model includes a probabilistic formulation to estimate route discovery failure. Simulations are performed to complement the analytic model. Results show that this attack can be kept in control with minimal harm on the network, provided that there is a detection mechanism; otherwise, with the increasing rate of compromised nodes, the harm on network tends to increase. As an interesting side result, our analysis also shows that our attack model can also be used to improve the performance DSR route discovery mechanism.

Similarly, Bhargava & Agrawal (2001) uses, ad hoc networks in a new generation of networks offering unrestricted mobility without any underlying infrastructure. Primary applications of ad hoc networks are in military, tactical and other security-sensitive operations, where the environment is hostile. Hence, security is a critical issue. Due to the nature of ad hoc networks, conventional security measures cannot be used. New security techniques are essential for a high-survivability network. The performance of the protocol may be severely affected in the presence of compromised nodes that inflict unpredictable and undetectable Byzantine
failure. We have identified certain misbehaviors caused by a malicious node to a reactive routing protocol, specifically the ad hoc on-demand distance vector (AODV) protocol. We also discuss the intrusion detection and intrusion prevention model to prevent several identified attacks in the network.

Subsequently, Islam et al (2005) due to the nature of the wireless media, ad-hoc wireless networks are vulnerable to various attacks. There are security protocols that prevent unauthorized nodes from accessing the network through authentication. Secrecy of information is provided through encryption. However these protocols cannot detect if any member of the network degrades the network performance due to misbehavior. Therefore an intrusion detection system (IDS) is required that monitors what is going on in the network, detects misbehavior or anomalies based on the monitored information and notifies other nodes in the network to take necessary steps such as to avoid or punish the misbehaving nodes. In this work we propose an IDS, referred to as the SAHN-IDS, suitable for multi-hop ad-hoc wireless networks like a SAHN (suburban ad-hoc network). SAHN-IDS detects misbehavior based on nodes getting an unfair share of the transmission channel. It also detects anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets. Unlike most IDSs for detecting anomalies in packet forwarding, SAHN-IDS does rely on overhearing packet transmissions of neighboring nodes, since that is ineffective in networks where nodes use different transmission power, different frequency channels and directional antennas for different neighbors. Moreover, unlike most IDSs, most of the thresholds in SAHN-IDS are set dynamically. We show the effectiveness of SAHN-IDS through simulations.

Vigna et al (2004) also uses a Mobile ad hoc network routing protocols are highly susceptible to subversion. Previous research in securing
these protocols has typically used techniques based on encryption and redundant transmission. These techniques prevent a range of attacks against routing protocols but are expensive to deploy on energy-constrained wireless devices. Experience in securing wired networks has demonstrated that, in addition to intrusion prevention techniques, it is useful to deploy intrusion detection techniques as a second line of defense. In this work, we discuss some of the threats to wireless ad hoc networks, and, specifically, some attacks against the AODV routing protocol. We also present a tool aimed at real-time detection of these attacks. The tool monitors network packets to detect local and distributed attacks within its radio range. Experiments show that the tool provides effective intrusion detection functionality while using only a limited amount of resources.

Puttini et al (2004) propose a new distributed intrusion detection system (IDS) designed for mobile ad hoc network (MANET) environments. The complete distribution of the intrusion detection process is the salient feature of our proposition: distribution is not restricted to data collection but also applied to execution of the detection algorithm and alert correlation. Each node in the MANET runs a local IDS (LIDS) that cooperates with others LIDS. A mobile agent framework is used to preserve the autonomy of each LIDS while providing a flexible technique for exploring the natural redundancies in MANET to compensate for the dynamic state of wireless links between high mobility nodes. The proposed solution has been validated by actual implementation, which is described in the work. Three attacks are presented as illustrative examples of the IDS mechanisms. Attack detection is formally described by specification of data collection, attack signatures associated with such data and alerts generation and correlation. Experiments exhibit fairly good results, the attacks being collaboratively detected in real-time.
Lu & Pooch (2002) studies the characteristics of mobile ad hoc networks (MANET) introduce vulnerabilities to malicious attacks varying from passive eavesdropping to active interfering. With routing being a critical aspect for MANET, routing security is drawing increased attention. Yet, to date there is little work published in this area. We propose a cooperative security-enforcement routing (CSER) protocol that intends to provide effective identification of misbehaviors on ad hoc routing, detection latency reduction and approximate location of the misbehaving node on a path. We introduce the concept of a security domain, which is composed of a set of hosts trusting each other and which can be assured a certain level of security. Our protocol requires that the nodes on a route from the same security domain cooperate as security monitor and enforcement points. Simulation results show that the protocol achieves good detection accuracy, lower detection latency and lower end-to-end delay than some other approaches. Planned future work is also described.

Sterne et al (2005) discuss the Intrusion detection in MANETs is challenging because these networks change their topologies dynamically; lack concentration points where aggregated traffic can be analyzed; utilize infrastructure protocols that are susceptible to manipulation; and rely on noisy, intermittent wireless communications. We present a cooperative, distributed intrusion detection architecture that addresses these challenges while facilitating accurate detection of MANET-specific and conventional attacks. The architecture is organized as a dynamic hierarchy in which detection data is acquired at the leaves and is incrementally aggregated, reduced, and analyzed as it flows upward toward the root. Security management directives flow downward from nodes at the top. To maintain communications efficiency, the hierarchy is automatically reconfigured as needed using clustering techniques in which cluster heads are selected based
on topology and other criteria. The utility of the architecture is illustrated via multiple attack scenarios.

Stakhanova et al (2006) presents the recent advances in intrusion detection field brought new requirements to intrusion prevention and response. Traditionally, the response to an attack was manually triggered by an administrator. However, increased complexity and speed of the attack-spread during recent years showed acute necessity for complex dynamic response mechanisms. Although intrusion detection systems are being actively developed, research efforts in intrusion response are still isolated. In this work we present taxonomy of intrusion response systems, together with a review of current trends in intrusion response research. We also provide a set of essential features as a requirement for an ideal intrusion response system.

Ganti et al (2002) discuss a data mining algorithm builds a model that captures interesting aspects of the underlying data. We develop a framework for quantifying the difference, called the deviation, between two datasets in terms of the models they induce. Our framework covers a wide variety of models including frequent item sets, decision tree classifiers, and clusters, and captures standard measures of deviation such as the misclassification rate and the chi-squared metric as special cases. We also show how statistical techniques can be applied to the deviation measure to assess whether the difference between two models is meaningful (i.e., whether the underlying datasets have statistically significant differences in their characteristics), and discuss several practical applications.

Similarly, Patwardhan et al (2005) proposed for secure routing and intrusion detection for ad hoc networks. Yet, little work exists in actually implementing such schemes on small handheld devices. In this work, we present a proof-of-concept implementation of a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent
intrusion detection system (IDS) for ad hoc networks. Security features in the routing protocol include mechanisms for nonrepudiation and authentication, without relying on the availability of a certificate authority (CA) or a key distribution center (KDC). We present the design and implementation details of our system, the practical considerations involved, and how these mechanisms can be used to detect and thwart malicious attacks. We discuss several scenarios where the secure routing and intrusion detection mechanisms isolate and deny network resources to nodes deemed malicious.

2.3 SUMMARY

This chapter discusses the importance and necessity for carrying out this research on intrusion detection problem on MANETs using various heuristic based methods. This chapter first reviews the literature pertaining to the present research and subsequently substantiates the need for various solution methods for solving the intrusion detection problem on MANETs.