A Survey of Intrusion Detection in Wireless Network Applications

Robert Mitchell and Ing-Ray Chen
Department of Computer Science
Virginia Tech
{rrmitche, irchen}@vt.edu

Abstract

Information systems are becoming more integrated into our lives. As this integration deepens, the importance of securing these systems increases. Because of lower installation and maintenance costs, many of these systems are largely networked by wireless means. In order to identify gaps and propose research directions in wireless network intrusion detection research, we survey the literature of this area. Our approach is to classify existing contemporary wireless intrusion detection system (IDS) techniques based on target wireless network, detection technique, collection process, trust model and analysis technique. We summarize pros and cons of the same or different types of concerns and considerations for wireless intrusion detection with respect to specific attributes of target wireless networks including wireless local area networks (WLANs), wireless personal area networks (WPANs), wireless sensor networks (WSNs), ad hoc networks, mobile telephony, wireless mesh networks (WMNs) and cyber physical systems (CPSs). Next, we summarize the most and least studied wireless IDS techniques in the literature, identify research gaps, and analyze the rationale for the degree of their treatment. Finally, we identify worthy but little explored topics and provide suggestions for ways to conduct research.

keywords: classification, intrusion detection, security, wireless networks

Acronyms

AODV	Ad hoc on demand distance vector
CDMA	Code division multiple access
CPS	Cyber physical system
DDoS	Distributed denial of service
DoS	Denial of service
DSR	Dynamic source routing
EER	Equal error rate
FN	False negative
FP	False positive
FSM	Finite state machine
GPRS	General packet radio service
GSM	Groupe spécial mobile
HIDS	Host based intrusion detection system
IDS	Intrusion detection system
LSASS	Local security authority subsystem service
LTE	Long term evolution
MANET	Mobile ad hoc network
MCPS	Medical CPS
MGCPS	Mobile group CPS
NIDS	Network based intrusion detection system
RSSI	Received signal strength indication
RTU	Remote terminal unit
SGCPS	Smart grid CPS
SNR	Signal to noise ratio
SVM	Support vector machine
TN	True negative
TP	True positive
UACPS	Unmanned aircraft CPS
UAV	Unmanned air vehicle
UMTS	Universal mobile telecommunications system
VANET	Vehicular ad hoc network
WISN	Wireless industrial sensor network
WLAN	Wireless local area network
WMN	Wireless mesh network
WPAN	Wireless personal area network
WSN	Wireless sensor network

1. Introduction

Intrusion detection is an important research topic with many potential applications. Along with intrusion prevention, response and tolerance, intrusion detection is one tool that can defend against the real-world cyber attacks threatening critical systems. These attacks include the Stuxnet attack on Iranian engineering facilities [1, 2], proof of concept attacks on insulin pumps [3] and cardiac devices [4], the DoS attack on a German power grid operator [5], the exfiltration attack on a Spanish power grid vendor [6, 7, 8] and the exfiltration attack on US UAVs [9, 10]. MGCPSs, MCPSs, SGCPSs and UACPSs are critical wireless network systems because of their human impact. For a battalion of 25 firefighters, failure of their MGCPS can

be fatal to the group or an individual. One of the primary functions of a first responder MGPCS is to provide situational awareness regarding hazardous materials. If the MGCPS does not identify a dangerous chemical in the environment and route that information correctly, the entire team is in jeopardy. For a hospital with 833 beds (e.g., Inova Fairfax Hospital), failure of their MCPS can be fatal to an individual. One of the primary functions of an MCPS is to administer analgesics. Overmedicating a patient will cause cardiac arrest. Another MCPS primary function is to provide cardiac support. Doing so when unnecessary or failing to do so when appropriate will kill the patient. While they are not life-critical, the scope of a SGCPS can be enormous. In July 2012, 620 million customers in India lost power for up to two days. A combat vehicle belonging to a UACPS could use weapons against noncombatants. In addition, a surveillance vehicle could fly into a densely populated area or critical resource (power substation, water treatment plant, center of government).

Malicious behavior damages the network by violating confidentiality, integrity, availability, authenticity, nonrepudiation or privacy; for example, a node in a mobile telephony network masquerades as another node in order to defeat the integrity of the billing function. *Selfish* behavior is a non-community minded action; for example, a node in a Mobile Ad Hoc Network (MANET) does not forward packets. Generically, we use the term *adversary* to refer to an undesirable node that exhibits selfish or malicious behavior. We make this distinction because it is critical to consider the attack model when evaluating a defensive technique.

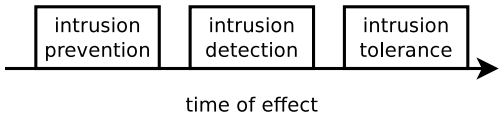

Figure 1: Spectrum of Network Security Measures.

Figure 1 shows the spectrum of network security measures, starting from intrusion prevention, then intrusion detection and as a last resort, intrusion tolerance. It is useful to think of network security measures in the time domain. The first opportunity a network operator has to defeat an adversary is when that adversary attempts to enter the network. An *intrusion prevention* measure stops the adversary at the network edge. One simple example is a group key users must provide to access the network. A more sophisticated example is an authentication scheme; this extends the group key concept to distinguish individual users. A third example is a survey tool that identifies vulnerabilities in system configuration that facilitate penetration [11].

Intrusion prevention is not effective against some attacks: any attack involving an insider/authenticated node, for example. An *intrusion detection* technique would find adversaries that have crossed the border of the network. One simple approach to find intruders is to look for nodes who have anomalous network traffic profiles.

Shin et al. [12] point out that intrusion detection is not effective against some attacks: any passive attack, such as eavesdropping, for example. Because intrusion detection cannot be 100% effective, robust systems must consider *intrusion tolerance* which seeks to survive and operate in the presence of adversaries who have penetrated the network and evaded detection. Intrusion tolerance measures can be static techniques that involve some form of redundancy; examples of static intrusion tolerance techniques are parallel or k-of-n designs. With these designs, if an attack causes an outage in one module, other modules can accommodate its load. Intrusion tolerance measures can also be dynamic techniques that involve a response at runtime; an example of dynamic intrusion tolerance is a load balancing mechanism.

When employing these network security measures, wireless IDSs must address several factors which distinguish them from wireline IDSs. First, wireless network nodes are more transient than their wireline counterparts; the wireless IDS threat model must encompass red (adversarial), blue (friendly) and green (nonaligned) nodes that come and go in seconds rather than weeks. Also, the wireless environment is rich with metadata that is not present in the wireline environment such as signal strength and clarity (SNR); this has two implications. The wireless IDS audit function must leverage features unique to the wireless environment, and it must poise for success by placing sensors in a way that establishes the most favorable geometry. Finally, the wireless IDS audit function must accommodate data sets that are incomplete due to network partition or affected by error (noise and bias). Data set noise sources include independent emitters (intentional jamming and benign channel competition), multipath interference (reflection in urban and subterranean environments) obstructions (terrain, vegetation and human made structures), atmospheric conditions (clouds and precipitation), variable signal strength (due to mobility and power control) and antenna placement (due to operational restrictions). Adversaries introduce bias into the data set; while this is the case in wireline networks, wireless adversaries are different than their wireline counterparts. Wireless adversaries can deny the physical medium to legitimate users by jamming and do not need physical access to a facility to attack [13, 14, 15, 16].

This survey paper is about intrusion detection. In particular, we classify existing IDS techniques in the literature, discuss their merits and drawbacks when applying to certain wireless systems, summarize strengths and weaknesses in intrusion detection research and suggest future research areas. The rest of the paper is organized as follows: Section 2 discusses the core functionality of intrusion detection in wireless environments. Section 3 provides a tree for organizing existing IDS protocols and explains the dimensions used for IDS classification. Section 4 surveys current intrusion detection literature and classifies existing

IDS techniques using the criteria from Section 3. Section 5 discusses lessons learned. Section 6 presents our conclusion and suggests future research directions.

2. Intrusion Detection Functions and Metrics in Wireless Networks

2.1. Core Intrusion Detection Functions

An IDS implements two core functions:

- collecting data regarding suspects
- analyzing the data

Examples of collection are: logging system calls on the local node, recording traffic received on a network interface and hearsay reputation scores (multitrust data or recommendations). Examples of analysis are: pattern matching, statistical analysis and data mining.

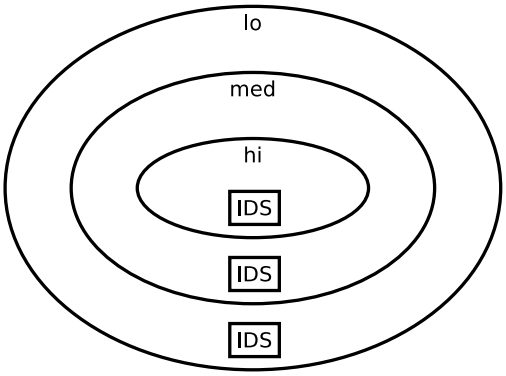

Figure 2: Defense In Depth.

The literature is abundant in these core functions. One common theme is that network defense should always have depth/be layered. These layers provide concentric zones with increasing levels security; the most sensitive data/functions are positioned within the innermost sectors. Figure 2 illustrates the concept of defense in depth [17]. Furthermore, there are situations where an inline/network gateway approach cannot effectively deal with even outside attackers: Inbound traffic on a wireless network is not confined to passing through a single point of presence. CPSs are large scale, geographically dispersed, federated, heterogeneous, life-critical systems that comprise sensors, actuators, control and networking components. First responder situational awareness systems, pervasive health care systems, smart grids and unmanned aircraft systems are some examples of CPSs. A CPS with federated control may have gateways to several agencies or organizations. Therefore, network defense should always have an all around scope/360 degree coverage. Figure 3 illustrates the concept of all around defense. In historical kinetic warfare, there is a "front line" that defensive resources are focused on; e.g., the Maginot Line of World War II. In modern kinetic warfare, there is no "rear security area" where forces can relax their guard; this concept translates directly to the cyber battlefield. A system manager cannot secure a resource by only applying security appliances to the public-facing interfaces (e.g., the web page). Rather, security appliances must be positioned at all entry points to the system (e.g., business/mission partner intranet links, telecommuter VPNs and WiFi access points).

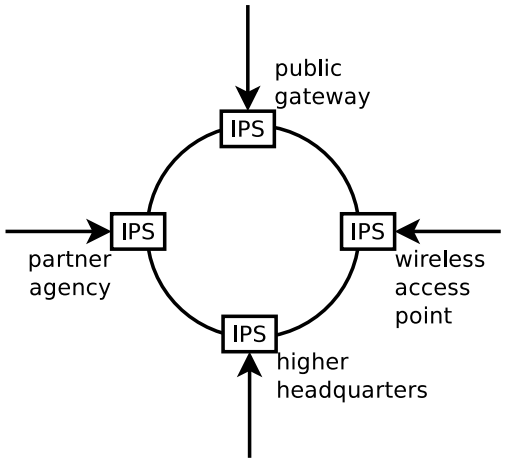

Figure 3: All Around Defense.

2.2. Intrusion Detection Performance Metrics

IDS researchers traditionally use three metrics to measure performance: false positive rate (FPR), false negative rate (FNR), and detection rate (DR) [11, 18, 19, 20, 21, 22, 23]. A false positive occurs when an IDS identifies a well-behaved node as an intruder; the literature also refers to this as a false alarm; specificity is the complement of false positive rate ($1 - FPR$). A false negative occurs when an IDS identifies a malicious or selfish node as well-behaved; the literature also refers to this as a failure to report [22, 23, 24]. On the other hand, a detection (a true positive) occurs when an IDS correctly identifies a malicious or selfish node [12, 18, 19, 20, 21, 25, 26]; true positive rate is synonymous with sensitivity and recall. Some researchers measure effectiveness using accuracy, which is calculated by $1 - FPR - FNR$.

Some research attempts to establish effective new metrics in order to enrich IDS research. Detection latency is a rarely used but critical means to measure IDS performance [27, 28]. Regardless of the attack model (passive or active), an earlier detection enables an earlier response. For target systems with resource limitations, power consumption, communications overhead and processor load are important metrics as well. There are several variations on this theme. Ma et al. [25] measure the time for an arbitrary number of nodes to exhaust their energy when using a given technique. Misra et al. [26] measure packet sampling efficiency. Packet sampling efficiency is the percentage of analyzed packets the IDS identifies as malicious;

the basic idea is that it is wasteful to sample lots of packets when only a few trigger an intrusion detection. Misra et al.'s design increases the sampling rate if the detection rate is above the penalty threshold and lowers the sampling rate if the detection rate is below the penalty threshold. Packet sampling efficiency must be balanced with detection rate. Packet sampling efficiency is directly related to penalty threshold, while detection rate is inversely related to penalty threshold. High packet sampling efficiency is good, but it cannot come at the expense of low detection rate. The critical problem here is separating low detection rates that come as a result of a placid environment using strong intrusion detection parameters and low detection rates that come as a result of relaxed intrusion detection parameters in a hostile environment. Farid and Rahman [21] measure time required to train their IDS and time required to analyze test data.

On the other hand, some studies attempt to establish metrics that are conceptually sound but have weaknesses in practice. Foo et al. [27] measure survivability as the ability of a system to serve customers and resist security violations. Shin et al. [29] and Bella et al. [30] use application-specific trust or reputation in their analysis; these metrics measure the goodness of nodes in terms of the specific business rules for a given purpose-built system. Furthermore, Shin et al. [29] supplement this statistic with quantity of invalid content distributed and fairness of load balance. It is not clear how researchers can apply these narrowly focused metrics to the research area as a whole. The relevance of survivability, application-specific trust and reputation are questionable as Foo et al., Shin et al. and Bella et al. leave their justification as open questions.

Finally, some studies attempt to establish metrics yet proven useful. Li et al. [31] borrow EER from the field of biometrics to measure performance; this is the rate at which false negatives (reject error) and false positives (accept error) are equal [32]. Li et al. make a strong assumption in asserting these rates are inversely related; if they are directly related, then EER is undefined because there could be many points where false negative and positive rates are equal. Haddadi and Sarram [33] test if a given IDS technique can detect each of a number of specific attacks. While this statistic is simple and elegant, it lacks context: it cannot tell a complete story.

3. Classification

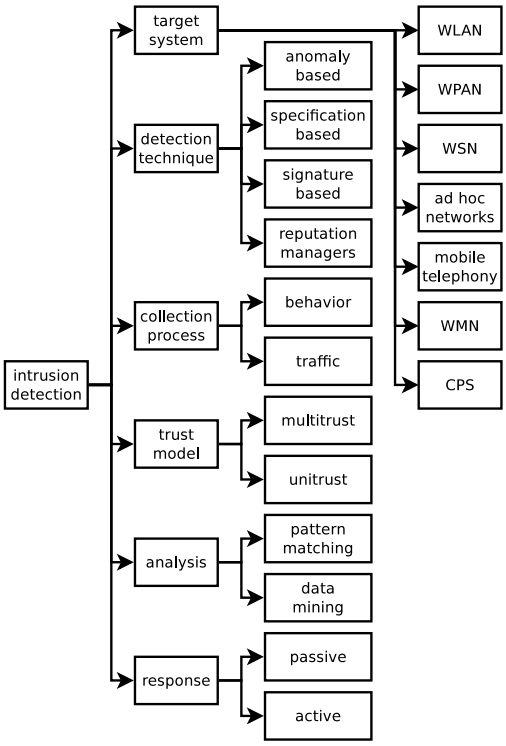

Figure 4: A Classification Tree for Intrusion Detection Techniques for Wireless Networks.

Figure 4 shows a classification tree for classifying existing IDS techniques in wireless networks. We classify the intrusion detection literature based on six criteria (or dimensions):

1. Target System: this criterion describes the intended environment for the IDS;
2. Detection Technique: this criterion distinguishes IDSs based on their basic approach to analysis;
3. Collection Process: this criterion contrasts behavior based IDSs from traffic based IDSs;
4. Trust Model: this criterion separates IDSs that share raw data or analysis results from standalone IDSs;
5. Analysis Technique: this criterion distinguishes simple pattern matching from sophisticated data mining approaches with regard to the particular implementation; while Detection Technique defines what the IDS looks for, Analysis Technique defines how the IDS looks for it;
6. Response Strategy: this criterion contrasts active from passive response strategies;

The classification tree organizes intrusion detection techniques in the literature to find gaps in IDS research and therefore identify research directions. Below we discuss each classification dimension in detail.

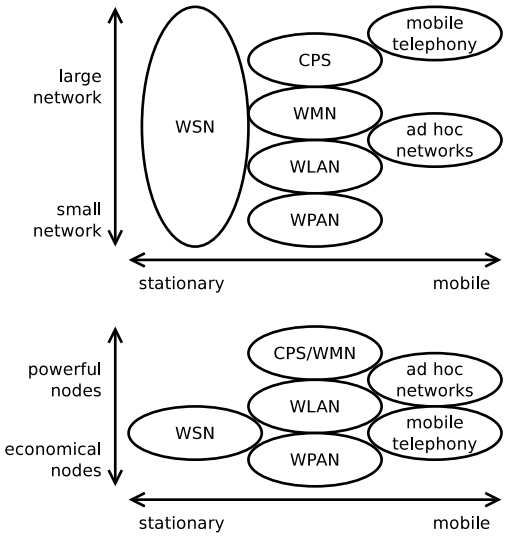

Figure 5: System Dimension of Intrusion Detection Literature.

3.1. Target System

The performance of any intrusion detection technique will vary based on its environment. IDS techniques have been developed for the following networking systems: WLANs, WPANs, WSNs, ad hoc networks, mobile telephony, WMNs and CPSs. Figure 5 shows the IDS "system" dimension characteristics of these networking systems in terms of network size (large versus small), mobility (stationary versus mobile) and capability (powerful versus economical). This figure expresses generalizations of each target system; counterexamples exist for some of these trends. Below we provide a brief overview of these networking systems.

3.1.1. Wireless Local Area Networks

WLANs use radios and protocols implementing the IEEE 802.11 series of specifications to network nodes within a 250 m range. Tao and Ruighaver [11] provide a comprehensive survey of intrusion detection that is specific to WLAN applications. The focus for WLAN IDSs is high detection rate. Detection of zero-day (unknown) attacks for nodes facing the Internet and self-tuning parameters for nodes administered by non-experts in unanticipated configurations are challenges shared with WPAN IDS. Interoperability, privacy requirements, undefined concept of operations, zero-day attack vulnerability and self-organization are WLAN features relevant to IDS. High interoperability and erratic profiles distinguish WLAN from other wireless applications.

3.1.2. Wireless Personal Area Networks

WPANs use radio communication to interconnect a handful of user operated devices within a 10 m range. Bluetooth and ZigBee are two widely adopted WPAN technologies. Interoperability, privacy and secrecy are key concerns in WPAN research. The focus for WPAN IDSs is low processor and memory burden. Detection of zero-day (unknown) attacks for nodes facing the Internet and self-tuning parameters for nodes administered by non-experts in unanticipated configurations are challenges shared with WLAN IDS. Energy conservation is not a major challenge for WPANs because they are attended networks where recharging is part of the concept of operations. Managing high false positives is not a major challenge for WPANs because they are attended, and a falsely evicted node can be rekeyed and returned to the network easily. Interoperability, privacy requirements, undefined concept of operations, zero-day attack vulnerability and self-organization are WPAN features relevant to IDS. WPANs differ from WLANs by radio range, protocol and form factor. Especially short wireless links distinguish WPAN.

3.1.3. Wireless Sensor Networks

WSNs are purpose-built systems whose scale spans a wide range. Deployments may comprise a large count of sensor nodes and a few base station nodes or only a modest number of sensor nodes with a single base station. We distinguish WSNs from WLANs and WPANs despite sharing physical and link layer protocols because WSNs are purpose-built, their energy is non-replenishable, they have unified administration (i.e., they are non-federated), they are unattended and they are free of infrastructure. The low-cost, unattended sensor nodes are equipped with sensors and/or actuators that run on battery and have strict size, weight and power requirements. The base station nodes have wired communications and unlimited power, and they may be attended. WSNs often extend off the shelf WPAN link layer technologies. Their typical indoor radio range is 10 m while their outdoor footprint can reach 100 m. Developing effective IDS techniques that can conserve energy of resource constrained sensors is one major challenge. Another major challenge is to dynamically control IDS settings to trade high false positives off for low false negatives to maximize the lifetime of a WSN. Drozda et al. [34] propose that if cascading classification is applied, it is possible to trade detection rate off for energy cost without an effect on false negatives. These authors also note that trading false positives off for low false negatives is tricky without a misclassification cost matrix, but with such a fixed matrix, this is straightforward. The focus for WSN IDSs is a low processor and memory burden. Highly redundant WSNs tolerate high false positive rates well. In some cases they are homogeneous systems with large degrees of sensor and radio overlap; these configurations fade gracefully when nodes fail (e.g., due to energy exhaustion, damage from a hostile environment or capture by an adversary). Three things distinguish WSNs from other wireless applications: First, processor, memory, energy and channel are scarce resources. Second, WSNs are usually not mobile; this limits the variability of the features mentioned in Section 1. Figure 5 generalizes here; while there are examples of mobile WSNs, they are not the general case [35]. Third, the rhythm of a WSN is

highly predictable: specifically, processing, memory, energy and channel will conform to a profile during normal operation. Hierarchical organization, tight concept of operations, non-replenishable energy, limited memory and processor and unattended operation are WSN features relevant to IDS.

3.1.4. Ad Hoc Networks

Ad hoc networks encompass MANETs and Vehicular Ad Hoc Networks (VANETs). MANETs are self-configuring mobile networks; they are open in the sense that there is no centralized management which increases flexibility. Like WSNs, they have no infrastructure requirement. The lack of centralized authentication blurs the concept of an intruder. Hence, some researchers argue that reputation management is a more natural fit than traditional intrusion detection. Likewise, tolerance measures with reform potential supplant eviction or other permanent sanctions. MANETs typically extend an 802.11 technology; therefore, their typical radio range is 250 m. The focus for ad hoc network IDSs is distributed design. Highly transient populations distinguish ad hoc networks from other wireless applications. Mobility, federation and lack of infrastructure are ad hoc network features relevant to IDS. Evicting detected nodes in ad hoc networks may be difficult or impossible so operating in their presence is a specific challenge for IDSs in ad hoc networks.

3.1.5. Mobile Telephony

Mobile telephony networks consist of many handsets and a few base stations. Consumers own and operate handsets which are inexpensive and widely available from many vendors. Service providers own and operate base stations which are significant investments. Base stations can be terrestrial (cellular networks) or overhead (satellite networks). Terrestrial examples of mobile telephony networks are: CDMA, GPRS, GSM, UMTS and LTE. Overhead examples of mobile telephony networks are: INMARSAT and Thuraya.

Mobile telephony radio ranges vary widely: terrestrial networks tend to be smaller while satellite networks tend to be larger. For example, a GSM microcell provides 2 km of coverage while a Thuraya spot beam provides 450 km of coverage [36]. Mobile telephony IDS techniques must not interfere with quality of service; specifically, the challenge here is to minimize false positives. False positives in mobile telephony result in a legitimate subscriber not using the network (i.e., not generating revenue). On the other hand, mobile telephony IDS techniques must establish nonrepudiation as regards billing; specifically, the challenge here is to minimize false negatives. Another challenge mobile telephony IDS techniques face is limited memory present in handsets and base stations; Section 3.2 will explain how this favors anomaly based approaches. Privacy is the final challenge to mobile telephony IDS techniques because of the tight coupling between a user and a handset. Geographic location and connection endpoints (e.g., websites visited, SMS sources and sinks and calling and called voice numbers) are rich sources of audit data, however it is Personally Identifiable Information (PII) and must be respected. Minimizing retained profile data is a complementary approach to meeting these last two challenges.

The focus for mobile telephony IDSs is high detection rate and low communications burden. These are concerns for the other target systems, but with mobile telephony they are especially important. A low detection rate results in intruders violating the nonrepudiation facet of their security; subscribers will protest their bills causing lost revenue due to non-payment and protest responses. A high communications burden limits the channel available for revenue generating flows. Especially long wireless links and federated control distinguish mobile telephony from other wireless applications. Terrestrial mobile telephony links span tens of kilometers while satellite links span thousands of kilometers. Mobile telephony control is federated among the corporate or government owned infrastructure and the many subscriber owned handsets.

Mobility, hierarchical organization, federation, limited memory and processor and privacy requirements are mobile telephony features relevant to IDS.

3.1.6. Wireless Mesh Networks

WMNs are highly-connected, purpose-built networks. The high degree of connection enables them to self-heal. In contrast with ad hoc networks, they are well-planned to balance cost, efficiency and reliability requirements. Nodes are typically stationary, although it is not uncommon for leaf nodes to be mobile. WMNs extend off the shelf link layer technologies such as mobile telephony, 802.11 (WLAN) or 802.16 (WiMAX); radio range varies accordingly (250 m to 50 km). Their high-connectedness and mission-orientation make WMNs an ideal application for IDS technology; the focus for WMN IDSs is high detection and low false positive rates. These are concerns for the other target systems, but they are especially important in WMNs. The ideal environment (e.g., tight concept of operation, high redundancy, relaxed memory and processor constraints and replenishable energy) leaves advancing the state of the art for the core metrics as the best line of investigation. High availability, plentiful resources and optimal antenna placement distinguish WMN from other wireless applications. Redundancy and tight concept of operations are WMN features relevant to IDS.

3.1.7. Cyber Physical Systems

CPSs have multiple control loops, strict timing requirements, a wireless network segment, predictable network traffic and contain legacy components. Some articles refer to this environment as a WISN [12]. CPSs fuse cyber (network components and commodity servers) and physical (sensors and actuators) domains. They use federated control due to stakeholders with different interests and concepts of operations. CPSs must self organize due to scale

and cannot be readily patched due to certification. They may contain human actors and mobile nodes. The term *Mobile CPS* indicates a CPS with mobile nodes. CPSs are trending towards heterogeneous, off-the-shelf components and open interfaces. CPSs may operate in locations that are dangerous due to heat, hazardous materials or violence. CPSs extend off the shelf link layer technologies such as WPAN, mobile telephony, 802.11 (WLAN) or 802.16 (WiMAX); radio range varies accordingly (10 m to 50 km). The attack model for a CPS encompasses short and long duration attacks. A reckless adversary can enter the network and immediately disrupts the concerned processes to cause a catastrophe. On the other hand, a more sophisticated adversary may take care to not disrupt normal system operation in order to propagate and set up a distributed attack launched at one point in time. This is the brand of attack Stuxnet used [1, 2]. For this reason, speed of detection is the key challenge in CPS IDS. It is worth mentioning that we have not found this metric being studied in the literature. The focus for CPS IDSs is leveraging unique CPS traits (sensor inputs, algorithms and control outputs) and detecting unknown attacks. Real-time requirements, tight concept of operations, legacy components and federation are CPS features relevant to IDS.

3.2. Detection Technique

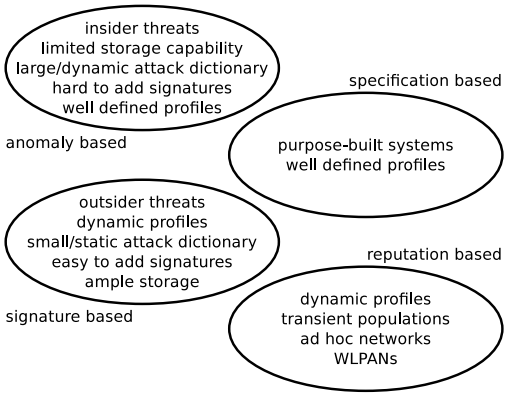

Figure 6: Detection Technique Dimension of Intrusion Detection Literature.

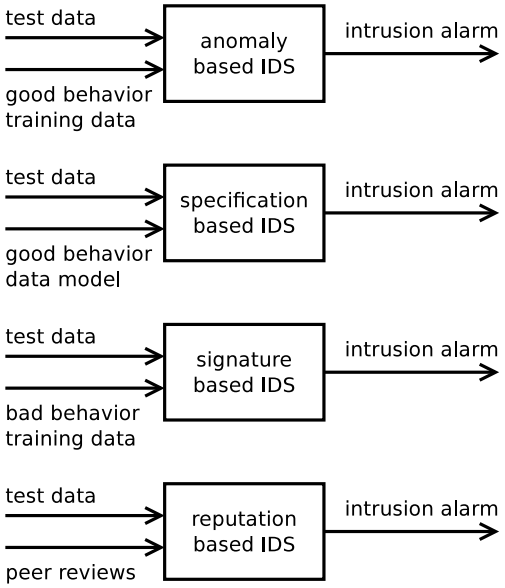

Figure 7: Comparison of Detection Techniques.

In this section, we first describe existing IDS detection techniques including anomaly based, signature based, specification based and reputation based techniques. Then we discuss the effectiveness of IDS detection techniques applying to various wireless networks discussed earlier in Section 3.1. Figures 6 and 7 show the detection technique dimension and compare the various detection techniques, respectively.

3.2.1. Anomaly Based Intrusion Detection

Anomaly based intrusion detection approaches look for runtime features that are out of the ordinary. The ordinary can be defined with respect to the history of the test signal (unsupervised) or with respect to a collection of training data (semi-supervised). Clustering is an example of unsupervised machine learning [37]. Beware some authors [19] refer to training data as a "signature." Some approaches, known as semi-supervised, train with a set of truth data. Other approaches, known as unsupervised, train with live data [38]. Researchers take different approaches for discrete, continuous and multivariate data sets. Examples of a discrete data set are dialed numbers or system state; Longest Common Subsequence (LCS) can be applied to discrete data over an interval while Hamming distance can be applied to discrete data instantaneously. Position and data rate is an example of a continuous data set; this type of data calls for a system of thresholds since exact matches will be rare. An example of a multivariate data set is a 3-tuple of position, RSSI and time; Machine learning approaches (e.g. genetic programming, clustering, neural networks and Bayesian classifiers) are useful for this brand of data.

The key advantage of anomaly based approaches is they do not look for something specific. This eliminates the need to fully specify all known attack vectors and keep

this attack dictionary current. One major disadvantage of this category is the susceptibility to false positives. For example, Hall et al. [20] investigated an anomaly based approach with a false positive rate as high as 100%. Another major disadvantage of this category is the training/profiling phase, during which the system is vulnerable. (This only applies to semi-supervised techniques.) Chandola et al. [39] provide a comprehensive survey of anomaly based intrusion detection that is general to all applications. White et al. [40] refer to anomaly based approaches as user or group profiling; Porras and Neumann [41] refer to this as a profile based approach.

Anomaly based approaches are further classified into conventional statistics based approaches and non-parametric methods. Data clustering and support vector machines (SVM) are examples of non-parametric methods [18]. A feature is a component of a multivariate data set (e.g., start time, end time, data source, data sink and position) [35]. The size of the feature set is a coarse indicator of efficiency for anomaly based approaches; larger feature sets suggest a larger memory requirement and higher microprocessor use. Xiao et al. [18] point out that feature selection is a key research problem with anomaly based approaches: more features do not necessarily give better results.

3.2.2. Specification Based Intrusion Detection

Specification based intrusion detection looks for abnormal performance at the system level; contrast this with anomaly based intrusion detection that analyzes specific user profiles or data flows. Specification based intrusion detection approaches formally define legitimate behavior and indicate an intrusion when the system departs from this model [42]. One major advantage of specification based intrusion detection is a low false negative rate. Only situations that violate what a human expert previously defined as proper system behavior generate detections. By definition, these approaches only react to known bad behavior; the theoretical basis is a bad node will disrupt the formal specification of the system. Another major advantage of specification based intrusion detection is the system is immediately effective because there is no training/profiling phase. The key disadvantage of specification based intrusion detection is the effort required to generate a formal specification. Specification based intrusion detection approaches are especially effective against insider attacks as they focus on system disruption. On the other hand, they are not the best approach for outside attackers because the specification (e.g., state machine or grammar) is application-specific and pertains to actions that only an insider can take. An outsider is not capable of generating transitions in the governing state machine or transforms in the defining grammar.

Specification based intrusion detection is a form of anomaly based intrusion detection where no user, group or data profiling is used. Instead legitimate behaviors are specified by humans and a nodes misbehavior is measured by its deviation from the specification. This allows for lightweight intrusion detection to be deployed in systems with severe resource constraints where user, group or data profiling is not possible.

3.2.3. Signature Based Intrusion Detection

Signature based intrusion detection approaches look for runtime features that match a specific pattern of misbehavior. Some sources refer to this approach as misuse detection [23, 27, 33, 43], supervised detection [44], pattern based detection [21] or intruder profiling [40].

One major advantage of this category is a low false positive rate. By definition, these approaches only react to known bad behavior; the theoretical basis is a good node will not exhibit the attack signature. The key disadvantage of this category is that the techniques must look for a specific pattern; a dictionary must specify each attack vector and stay current. An attack signature can be a univariate data sequence: for example, bytes transmitted on a network, a program's system call history or application-specific information flows (sensor measurements in a WSN or CPS). One sophistication is to combine simple data sequences into a multivariate data sequence [38]. The important research problem in this field is creating an effective attack dictionary [23]. Signature length is a coarse indicator of efficiency for signature based approaches; longer signatures suggest a larger memory requirement and higher microprocessor use. Signature based approaches are more effective against outsider attacks; malicious outsiders presumably will exhibit well known signatures in the course of penetrating the network.

3.2.4. Reputation Management

The primary function of a reputation manager is to detect nodes exhibiting selfish behavior rather than violating security. However, in the presence of malfeasance, reputation managers must also guard against colluding nodes intent on enhancing their reputation. Bella et al. [30] identify the main problem in MANET Reputation Management as distributing reputation scores. Reputation Management approaches are particularly applicable to large networks where establishing a priori trust relationships is not feasible. Examples of metrics reputation managers use are packets forwarded over packets sourced, packets forwarded over non-local packets received and packets sent over packets received. Choosing the metric is a matter of design philosophy. Using packets forwarded over non-local packets received mitigates a bias present in packets over packets sourced. Weighting data is a key problem for the analysis: data points have different significance across the time domain (recent data may be more or less valuable than historical) as well as across sources (experienced data is more valuable than observed data which is more valuable than multitrust data). Reputation management is especially relevant to ad hoc applications in MANETs and VANETs.

3.2.5. Effectiveness of Detection Techniques Applying to Wireless Systems

In this section, we reason why certain detection techniques are more effective than others when applying to certain wireless systems.

Anomaly based designs are more effective than the other designs for mobile telephony base stations, WMNs and attended CPSs. The common theme these systems share is a well defined concept of operations, i.e., they are mission-oriented/purpose-built and thus have predictable profiles. These systems also have unique aspects which favor anomaly based designs. For example, for WMNs the attack model must include insider threats against whom anomaly based designs are more effective. For attended CPSs, due to federated control and safety criticality, maintenance of attack dictionary updates (for signature based intrusion detection) is difficult. For wireless systems that favor anomaly based designs, their ability to detect unknown attacks offsets their higher false positive rate and computational complexity.

Signature based designs are more effective than the other designs for WLANs, WPANs and mobile telephony handsets. The common themes these systems share are an ill-defined concept of operations/unpredictable profiles and ease of maintenance (that is, attack dictionary updates). Maintenance is easy for WLANs and WPANs because of their human attendant. The large storage capacities of WLANs also facilitates attack dictionary management. Maintenance is easy for mobile telephony handsets because of their high connectivity and human attendant. In addition to other shared themes, WLANs and WPANs favor signature based designs because of their concern for outsider threats. For wireless systems that favor signature based designs, their low false positive rate offsets their inability to detect unknown attacks and large storage requirement.

Specification based designs are more effective than the other designs for WSNs and unattended CPSs because of their predictable profiles and limited resources (storage and channel). The channel scarcity does not accommodate dictionary updates and the limited storage limits the size of the attack dictionary. For wireless systems that favor specification based designs, neither anomaly nor signature based designs are viable due to computational or storage limitations; a specification based design offers an effective way for them to provide security. Because of high sensor redundancy, false positives are less important than false negatives in WSNs; they can tolerate unwarranted sensor evictions in the same fashion as sensors exhausting their energy or succumbing to its hostile environment.

Reputation management designs are more effective than the other designs for ad hoc networks. The ill defined concepts of operations of ad hoc networks reduce the effectiveness of anomaly based designs. Maintenance difficulty, due to lack of connectivity, reduces the effectiveness of signature based designs. Their egalitarian nature makes ad hoc networks an ideal application for reputation management designs. These unique conditions led to the innovation of reputation managers for these systems. Reputation managers are not a good choice for hierarchical networks if they have a tightly specified communication infrastructure that cannot accommodate the associated gossip. Wireless systems that favor reputation based designs are highly federated (lack central authority) and have highly transient populations.

3.3. Collection Process

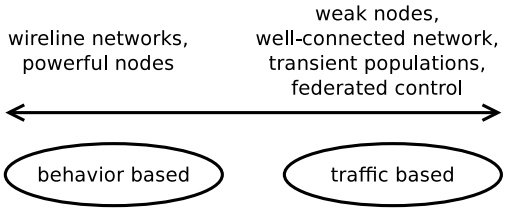

Figure 8: Collection Process Dimension of Intrusion Detection Literature.

Figure 8 shows the data collection dimension for classifying IDS approaches. There are two ways to collect data before data analysis, namely, behavior based collection and traffic based collection. We first describe the essentials of behavior and traffic based collection. Then we discuss the effectiveness of behavior and traffic based collection in various wireless systems. It is clear that both collection processes are important from the perspective of attack detection when there are attacks on both hosts and networks that join them.

3.3.1. Behavior Based Collection

IDSs using behavior based collection analyze logs maintained by a node or other audit data, such as file system details, to determine if it is compromised. One major advantage of using behavior based collection approaches is scalability; this is attractive for large scale applications like WSN and mobile telephony. Another major advantage of using behavior based collection approaches is decentralization; this is attractive for infrastructure-less applications like ad hoc networks. One major disadvantage of a behavior based collection is each node has to perform additional work to collect, if not analyze, their audit data. This is relevant in resource constrained applications like WSN and mobile telephony. Another major disadvantage of this technique is that a sophisticated attacker can cover their tracks by modifying the audit data on the captured node. A third disadvantage of this technique is that it can be OS or application specific (depending on the particular content of the logs) [23]. Behavior based collection is not used widely in wireless environment applications [11].

3.3.2. Traffic Based Collection

IDSs using traffic based collection study network activity to determine if a node is compromised. This audit can

be general (traffic/frequency analysis) or protocol-specific (deep packet inspection). The key advantage regarding resource management is that individual nodes are free of the requirement to maintain or analyze their logs. The key disadvantage regarding data collection is that the effectiveness of a traffic based technique is limited by the visibility of the nodes collecting audit data. Thus, it is challenging to arrange traffic based collection sensors to get complete intra-cell and inter-cell pictures of network activity [11].

3.3.3. Effectiveness of Collection Processes Applying To Wireless Systems

In this section, we reason why certain collection processes are more effective than others when applying to certain wireless systems.

Traffic based collection typically is more effective than behavior based collection for most wireless systems. WLANs, WPANs and ad hoc networks have transient user populations, making it hard for a node to collect behavior data of a suspect roaming in the system. WSNs and mobile telephony handsets have limited storage, making behavior based collection impractical. While it does not have obvious benefits for the collection function, WMNs should employ traffic based collection, as their high degree of connectivity results in a great data set for traffic based analysis when using this process. CPSs are under federated control, so administrative concerns may prevent an intrusion detector in one segment from accessing user logs in another segment. In many situations, the wireless environment benefits audit data collection by providing features that are not present in the wireline environment; for example, an IDS that uses traffic based collection to record signal strength from a set of well positioned sensors has a powerful data set.

Behavior based collection typically is not more effective than traffic based collection in a wireless system. One rare example is that mobile telephony base stations favor behavior based collection because they use wireline communication and have large storage capacities. In some situations, the wireless environment disrupts, rather than enriches audit data collection; for example, if the RF interference is too great or node geometry is too unfavorable, behavior based collection is a better choice than traffic based collection.

Here we should note that some papers use the terms HIDS and NIDS when referring to behavior based collection and traffic based collection, respectively [43, 45, 46].

While certain wireless systems may favor one or the other, both traffic and behavior based collection processes are important from the perspective of attack detection when there are both network and host centric attacks. The adversary chooses the attack vector; "the enemy has a vote" as warfighters say. Security appliances must organize their defense based on the threat model and not merely based on what is convenient.

3.4. Trust Model

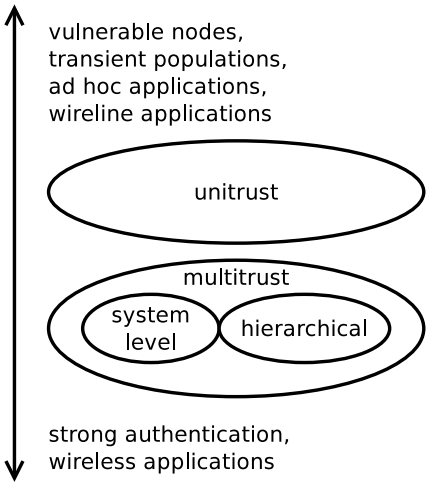

Figure 9: Trust Model Dimension of Intrusion Detection Literature.

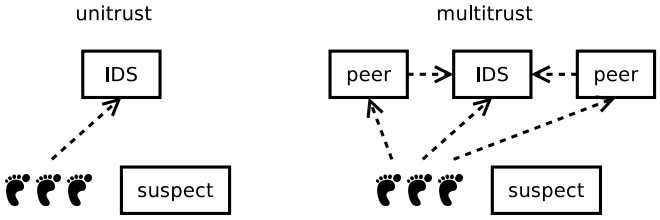

Figure 10: Comparison of Trust Models.

Figures 9 and 10 show the trust model dimension for classifying IDS approaches and the comparison of trust models, respectively. The trust model dictates what data a monitor node uses to audit trustee nodes. Experienced data, which is a firsthand account, is highly trusted. Reported data, which is a thirdhand account, is least trusted; bad nodes can "ballot stuff" for their confederates and badmouth the good actors. Observed data falls between experienced and reported data in credibility. It is available for any trustee to audit, but colluding adversaries can create acts of "reputation theater" to boost their reputation [47]. There are two basic trust models, namely, multitrust and unitrust. We first describe the essentials of multitrust and unitrust. Then we discuss the effectiveness of multitrust and unitrust in various wireless systems.

3.4.1. Multitrust

Multitrust is the concept of using hearsay/reported information (data from witnesses or third parties). Liu and Issarny [48] call this type of information a *recommendation*. Contrast recommendations with what Shin et al. [12] call *direct monitoring*. This hearsay information can be raw data or an analysis result. Using multitrust together with behavior based collection mitigates a key weakness: the opportunity for capable adversaries to

cover their tracks. Multitrust often appears in the context of reputation management which is most applicable to ad hoc applications such as MANET and VANET. However, giving weight to others' recommendations in a federated environment leads to a dilemma: On one hand, a node places enough trust in neighbors to include their hearsay in reputation calculations. On the other hand, nodes are suspicious enough of their environment to measure and respond to the reputation of their neighbors. Therefore, multitrust is better suited to increasing the security of managed/authenticated environments rather than to establishing a basic level of security in ad hoc environments such as MANETs or VANETs.

Reputation managers require two levels of trust: the "outer circle" of trust regards the system function in general while the "inner circle" of trust regards the multitrust function specifically. The literature uses the term *trustworthiness* in reference to this "inner circle" credibility [29]. Because the effectiveness of traffic based approaches are limited by radio range in wireless environments, multitrust offers an advantage for these applications. The literature sometimes calls multitrust approaches cooperative; it further distinguishes them as distributed or hierarchical [12].

3.4.2. Unitrust

We classify some IDSs as unitrust, which some research refers to as standalone. In contrast with multitrust designs, a unitrust design does not use reported information; a unitrust design relies on direct monitoring. The advantage of a unitrust design is the data is completely reliable; the IDS does not need to apply safeguards to prevent or tolerate biased reports from adversaries. The disadvantage of a unitrust design is the smaller data set; the IDS only acts on the data it experiences or observes.

3.4.3. Effectiveness of Multitrust versus Unitrust Applying to Wireless Systems

In this section, we discuss the effectiveness of multitrust vs. unitrust as applying to various wireless systems. Here we should note that the discussion is based on the assumption that only multitrust or unitrust is being used. We recognize that many reputation and trust management systems actually take into consideration of both multitrust and unitrust in trust composition [49, 50, 51, 52, 53, 54, 55, 56, 57].

Multitrust is more effective than unitrust for mobile telephony and WMNs. The common theme these systems share is a high level of trust. In mobile telephony, this high level of trust follows from their strong authentication; billing accuracy requires this strong authentication to be in place. In WMNs, stationary infrastructure nodes are inherently trustworthy while mobile terminal nodes are not. These wireless systems must use a trusted agent/authenticator to broker multitrust data in order to guarantee its provenance. The majority of contemporary reputation systems are based on multitrust because of the benefits of multitrust over unitrust in making use of the existing multitrust knowledge for intrusion detection. Wireless systems with highly transient populations can make the most use of multitrust designs.

Unitrust is more effective than multitrust for WLANs, WPANs, WSNs, ad hoc networks and CPSs. The common theme these systems share is difficulty in establishing trust. For WLANs, WPANs and ad hoc networks, this is due to the transience of the terminal nodes. For WSNs, this is due to the vulnerability of sensor nodes to capture because they are unattended. For CPSs, this is due to federated control of CPSs; authentication may not span segments of the CPS. In general, the lack of trust and authentication in these systems makes multitrust difficult. However, one drawback of a unitrust approach is the loss of additional situational awareness a multitrust system can offer. As one example, a newly arrived intrusion detector will not have any audit data that preceded its arrival. As another example, an unfavorably located intrusion detector on a wireless network will not have any audit data transmitted beyond its radio range. In these examples, the intrusion detector will use an unnecessarily small set of audit data. In spite of WLANs, WPANs, WSNs, ad hoc networks and CPSs favoring unitrust in some ways, multitrust reputation systems allow an entity entering the network to use the existing knowledge in trust to deal with incomplete and uncertain information. Wireless systems with highly persistent populations, good visibility and minimal trust will favor unitrust designs.

3.5. Analysis Technique

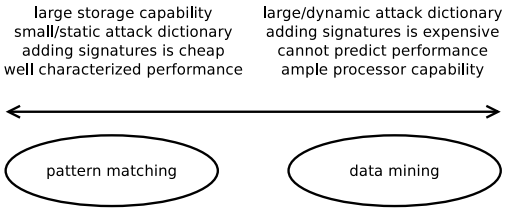

Figure 11: Analysis Dimension of Intrusion Detection Literature.

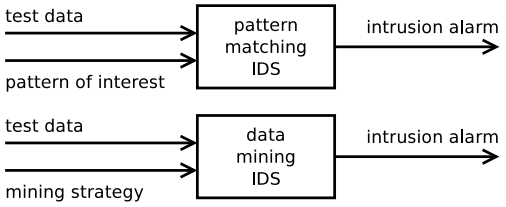

Figure 12: Comparison of Analysis Techniques.

Figures 11 and 12 show the analysis dimension for classifying IDS approaches and the comparison of analysis techniques, respectively. We first describe the essentials of pattern matching and data mining. Then we discuss

the effectiveness of pattern matching and data mining in various wireless systems. Analysis is the second of the two core IDS functions discussed in Section 2. There are two ways to analyze data, namely, pattern matching and data mining; we classify analysis techniques along these lines.

3.5.1. Pattern Matching Analysis Techniques

A pattern matching approach simply scans an input source. Signature based approaches [18, 22, 23, 24, 26, 33, 40, 41, 58, 59, 60, 61, 62, 63, 64] scan for entries in the attack dictionary (known bad profiles). Semi-supervised anomaly based approaches scan for deviations from expected performance (known good profiles). Reputation based approaches [30, 47, 65] scan profile data to measure some criteria established prior to deployment.

3.5.2. Data Mining Analysis Techniques

The unsupervised variants of anomaly based IDSs are examples of data mining [20, 21, 31, 44].

3.5.3. Combined Analysis Techniques

[19, 23, 43] blend both pattern matching and data mining techniques. Machine learning techniques blur the line between pattern matching and data mining approaches. Specifically, the literature contains research applying genetic programming, clustering (as regards data mining), neural networks and Bayesian classifiers [21] to intrusion detection. Some research focuses analyzing the audit data [12, 25, 26, 27, 66, 67, 68]. These studies treat the analysis function as a black box while proposing data collection innovations.

3.5.4. Effectiveness of Analysis Techniques Applying to Wireless Systems

In this section, we reason why certain analysis techniques are more effective than others when applying to certain wireless systems.

No target system clearly favors pattern matching or data mining. Wireless network nodes and WMNs have large storage capabilities and can update their attack dictionaries easily, which are conducive to pattern matching. However, their ill defined concepts of operations/unpredictable profiles are conducive to data mining. WSNs have well defined concepts of operations, which are conducive to pattern matching. However, their limited storage capabilities and maintenance difficulty are conducive to data mining. Ad hoc networks have large storage capabilities which are conducive to pattern matching. However, their ill defined concepts of operations/unpredictable profiles and maintenance difficulty are conducive to data mining. Mobile telephony handsets can update their attack dictionaries easily, which is conducive to pattern matching. However, their limited storage capabilities and ill defined concepts of operations/unpredictable profiles are conducive to data mining. CPSs have large storage capabilities and well defined concepts of operations, which are conducive to pattern matching. However, their maintenance difficulty is conducive to data mining. Consequently, the literature is abundant in adopting both pattern matching and data mining techniques [19, 23, 43]. Wireless systems with minimal computational resources and a static attack model will favor pattern matching. Wireless systems with sufficient computational resources can benefit from data mining by evolving to address a dynamic adversary.

4. Classifying Existing Intrusion Detection Techniques

This section applies the criteria Section 3 established to the current research on intrusion detection in wireless environments. We survey 60 existing IDS techniques in the literature and classify them according to the classification tree in Figure 4. The intent is to examine the most and least intensive research in IDS to date and identify research gaps yet to be explored. We summarize our findings in Tables 1-7 based on the "system" dimension of IDS techniques. Table 8 classifies generic IDS techniques without any system designation.

4.1. WLANs

We apply the classification tree to organize six IDS technique in WLANs and summarize the results in Table 1.

4.1.1. Anomaly Based Designs

Zhong et al. [44] use an online k-means algorithm to cluster network traffic to detection intruders. Specifically, their criteria is the suspect's distance from the largest cluster. The pro of this study is: finding that nominal features (for example, wireless access point (WAP) identifier), instead of numerical features (ordinal, interval or ratio) confuses results. The cons of this study are: marginal detection rates (65.3 to 82.5%) and strong assumptions (the majority of network activity is normal and the normal activity clusters tightly). The authors detect nodes that source an abnormally high number of packets: these could be probing or DoS attacks.

The anomaly based IDS in [59] that relies on RSSI is one example of using raw multitrust data to detect anomaly behaviors. The pro of this study is that it improves performance by using multitrust data from untrusted nodes. The con of this study is that it does not accommodate mobility. Their approach focuses on spoofing attacks.

4.1.2. Anomaly + Signature Based Designs

Hairui and Hua [58] address lack of IDS interoperability with Multi-agent Based Distributed WLAN IDS (MABDIDS). In their two-tier analysis function, the Data Analysis Agent performs coarse detection while the Management Agent performs fine detection based on the initial

Table 1: Classification of WLAN IDSs

	detection technique	collection approach	multi-trust	analysis
Zhong Technique [44]	anomaly	traffic		data mining
Nodeprints [59]	anomaly	traffic	yes	pattern matching
MABDIDS [58]	anomaly + signature	behavior + traffic	yes	pattern matching
Haddadi Technique [33]	anomaly + signature	traffic		pattern matching
Yuan Technique [69]	anomaly + signature	traffic		data mining
Sneeze [70]	signature	traffic		pattern matching

findings of Data Analysis Agents. The response agents (Data Analysis and Management) can coordinate to efficiently and effectively collect more extensive data on possible intruders. The pro of this study is a fully distributed design. The con of this study is a lack of numerical results. The authors do not tie their IDS to any attack type.

Haddadi and Sarram [33] propose a combined anomaly and signature based IDS using traffic based collection. In their two-tier analysis function, signature and anomaly detection modules run in parallel to form the first stage. If they cannot classify the data as an attack or normal, they forward the audit data to a second stage a probable attack detection module for review. The pro of this study is that it uses a realistic data set for testing. The con of this study is a lack of numerical results. The authors focus on man in the middle and DoS attacks.

Yuan et al. [69] use an immunological approach inspired by danger theory and dendritic cells (a type of antigen presenting cell) to create a four-layer IDS. They combine signature and anomaly based detection techniques. Yuan et al.'s approach is informed by danger theory in the sense that it detects damage rather than the adversary itself. One key idea is that dendritic cells are ineffective initially but learn to be effective after exposure to adversaries; this is analogous to an unsupervised anomaly based detection technique. The authors establish the immunological metaphor by mapping antigens, dendritic cells, signals, immune memory and immune response to network traffic, detectors, detector and correlation output, an attack dictionary and danger handling, respectively. The authors focus on zero-day (unknown) attacks: specifically, the KDD Cup 1999 data set. This paper relies on the Dendritic Cell Algorithm (DCA) that seems to be a population of linear classifiers, as observed by Stibor et al. [71].

4.1.3. Signature Based Designs

Sampangi et al. [70] propose the Sneeze algorithm to detect intruders on a WLAN and locate them. Their approach is biomimetic in the sense that it detects and expels an intruder at the network edge in the same fashion an organism's respiratory system does to a foreign body at the nose in the course of sneezing. The BSSID/MAC of every valid access point is on a whitelist. The basic idea is that APs monitor one another by searching for unrecognized BSSID/MACs. If an AP running Sneeze finds an unrecognized BSSID/MAC, it rekeys and notifies the system administrator. The response (sneeze-analog) has two aspects: rekeying and a human searching the area surrounding the reporting AP and removing the rogue AP. Sneeze is essentially a signature based detection technique with a traffic based collection process and simple pattern matching. The authors focus on attacks involving a rogue access point/man in the middle.

4.2. WPANs

We apply the classification tree to organize three IDS techniques in WPANs and summarize the results in Table 2.

4.2.1. Anomaly Based Designs

Yang, et al. [72] studied Grid-based clustering over K-neighborhood (GREEK) which is targeted for WPAN (ZigBee, specifically) applications. The authors use an anomaly-based detection technique, a traffic-based collection approach and data mining (clustering, specifically) analysis. Their attack model considers only physical intruders. Yang, et al. collected data empirically. While the authors did report numerical results related to the efficiency of data mining, they did not report data related to intrusion detection (for example, true positive or false positive rate).

4.2.2. Anomaly + Signature Based Designs

Moyers, et al. [73] studied Multi-Vector Portable IDS (MVP-IDS) which is targeted for WPAN applications. The authors use a combined anomaly and signature-based detection technique, a combined behavior (battery current, specifically) and traffic-based collection approach and pattern matching analysis. Their attack model considers resource depletion attacks. While Moyers, et al. did claim one MVP-IDS module [Bluetooth Attack Detection and Signature System (BADSS)] achieved a 100% detection rate with only a 2.97% false positive rate, the authors did not provide numerical results on key metrics for the complete system.

Table 2: Classification of WPAN IDSs

	detection technique	collection approach	multi-trust	analysis
GREEK [72]	anomaly	traffic	yes	data mining
MVP-IDS [73]	anomaly + signature	behavior + traffic		pattern matching
Bluetooth IDS [74]	signature	traffic		pattern matching

4.2.3. Signature Based Designs

OConnor and Reeves [74] studied Bluetooth IDS which is targeted for WPAN (Bluetooth, specifically) applications. The authors use a signature-based detection technique, a traffic-based collection approach and pattern matching analysis. Their attack model includes scanning, DoS and exfiltration. OConnor and Reeves collected data empirically using four different Bluetooth devices as victims. The authors only reported numerical results for detection latency.

4.3. WSNs

We apply the classification tree to organize 14 IDS techniques in WSNs and summarize the results in Table 3.

4.3.1. Anomaly Based Designs

Da Silva et al. [75] propose a centralized IDS that uses traffic based collection. The authors apply seven types of rules to audit data: interval, retransmission, integrity, delay, repetition, radio transmission range and jamming. The pro of the study is their design's modest energy demand. The cons of the study are performance (detection rates as low as 30% and false positive rates as high as 50%) and the inability to detect unknown attacks. The authors consider message delay, replay, wormhole, jamming, data alteration, message negligence, blackhole and greyhole attacks.

Drozda et al. [34] pursue a biology-inspired intrusion detection approach targeted for WSN applications. This is a semi-supervised anomaly-based design. The authors used JiST/SWANS to simulate a network with 1718 nodes exchanging traffic at a low, constant bit rate (272 bps). Their attack model includes greyhole attacks and attacks where the adversary chooses random packets to delay for a random time interval. Drozda et al. configure the subject WSN with 236 bad nodes (14%). Their data indicates detection rate for their technique ranges from 41.14 to 99.94% and false positive rate ranges from 2.22 to 62.07% depending on window size and number of rounds.

Rajasegarar et al. [76] study an anomaly-based IDS for WSN applications called Elliptical Anomaly (EA). Their approach is distributed, and they claim it provides the same accuracy as a contemporary centralized approaches while using less energy and exhibiting a lower detection latency. The energy savings stems from the reduction in audit data passed over the network. Data transmission typically dominates the energy usage of a WSN node, so they correctly reason the additional microprocessor load is justified. The authors provide detection rate and false positive rate data supporting their accuracy claim but do not show evidence to support their energy efficiency or detection latency claims. Specifically, the authors pit EA against Nearest Neighbor (NN), Kth Nearest Neighbor (KNN), Average of K Nearest Neighbors (AvgKNN) and Distance Based Outliers (DBO) techniques. The authors use empirical data from four data sets: Intel Berkeley Research Laboratory (IBRL) Great Barrier Reef (GBR) Great Duck Island (GDI) and a data set they synthesized.

Xiao et al. [18] propose a semi-supervised IDS called Machine Learning (ML) that uses a Bayesian classifier. ML performs detection on each sensor node in order to remove data before it taints the network data flow via aggregation or other in-network processing. They adapt machine learning to the resource constraints of a WSN by limiting the feature set to three parameters. Network related (for example, packet collisions) or host related (for example, power consumption) data can drive their classifier. The pros of this study are numerical results and comparative analysis with contemporary approaches TPDD and DAD. The con of this study is the weak attack model; the authors only consider packet replay attacks.

Mao [60] proposes a multitrust design for heterogeneous WSNs formed by four layers: network, semantic, model and cooperative. The author refers to sensors that participate in the IDS as agents and to other sensors that do not participate in IDS as common nodes. Agents form a multitrust relationship within and between groups to perform anomaly based IDS functions. The pro of this study is the finding that an agent to common node ratio of 1:1 effectively trades cost and effectiveness. The author does not tie the proposed IDS to any attack type.

4.3.2. Anomaly + Signature Based Designs

Misra et al. [26] create Simple LA Based Intrusion Detection (S-LAID) by extending Learning Automata based protocol for Intrusion Detection (LAID) to WSNs by making it more efficient and energy aware; the learning automata select optimal points in the WSN to hunt for intruders. The authors balance energy efficiency and detection effectiveness by changing the fraction of inbound packets sampled based on detection rate; the basic idea is to spend constrained resources liberally when the environment is hostile and to conserve those resources otherwise.

Table 3: Classification of WSN IDSs

	detection technique	collection approach	multi-trust	analysis
da Silva Technique [75]	anomaly	traffic		pattern matching
Drozda Technique [34]	anomaly	traffic		data mining
EA [76]	anomaly	behavior		data mining
ML [18]	anomaly			pattern matching
Mao Technique [60]	anomaly		yes	pattern matching
S-LAID [26]	anomaly + signature	traffic		pattern matching
Ma Technique [25]	anomaly + signature			
ATRM [77, 78]	reputation	behavior	yes	
Hur Technique [79]	reputation	traffic		pattern matching
RFSN [80]	reputation	traffic	yes	
TTSN [81]	reputation	traffic		
Onat and Miri Technique [35]	signature	traffic	yes	
Zamani Technique [82]	signature	traffic	yes	
Ioannis Technique [83]	specification	traffic	yes	

The pro of this study is a fully distributed design. The con of this study is the attack model which considers the integrity and availability dimensions of security; it does not consider confidentiality, privacy or non-repudiation. The authors focus on data manipulation attacks.

Ma et al. [25] propose a non-cooperative game theory based IDS which models income for the cluster head and the attacker: cluster head income is a function of the cost of running the IDS, the utility of the cluster head and whether the cluster head is under attack while attacker income is a function of the cost of effecting the attack, the utility of the attack target and whether the target is running the IDS. The authors assume a cluster based network topology and sensors in the WSN are stationary and homogeneous; only cluster heads run the IDS. The con of this study is the detection rate, which is as low as 70%. The authors consider jamming, exhaustion, routing and flooding attacks.

4.3.3. Reputation Based Designs

Boukerche et al. [77, 78] propose an IDS called Agent based Trust and Reputation Management (ATRM) that relies on a piece of trusted software, a Trust and Reputation Assessor (TRA), running on all nodes. Sensors exchange trust instruments and reputation certificates. The pros of this study are a fully distributed approach and minimal communication overhead and energy use. The con of this study is a strong assumption that the mobile agent always operates correctly, even on a captured node.

Hur et al. [79] propose an IDS that crosschecks redundant sensor readings. Clusters select an aggregator, which forwards sensor data to the sink, based on trustworthiness scores. The pro of this study is the detailed treatment of the trustworthiness formula which is based on: distance, quantity and quality of data produced and energy remaining. The con of this study is that their threat model does not consider cooperating malicious nodes. The authors focus on data manipulation attacks.

Ganeriwal et al. [80] propose an IDS called Reputation based Framework for Sensor Networks (RFSN) that calculates reputation scores based on similarity of data reported by sensors with overlapping coverage. RFSN uses density based outlier detection to generate reputation scores, integrates reputation scores into a trust score using a Bayesian formulation and lowers trust scores over time if they are not refreshed. The pro of this investigation is the experimental design: the authors simulate their design, implement it and collect data in both lab and operational environments.

Chen [81] proposes an IDS called Task based Trust framework for Sensor Networks (TTSN). TTSN manages reputation on a per task (for example, sensing, packet forwarding, cluster management, time synchronization and localization) basis for each sensor rather than using a single metric for each node. TTSN uses an aging factor, γ to weight the per task reputation score. The pro of this study is comparative analysis with contemporary approaches ATSN and RFSN. The con of this study is a lack of numerical results: aggregate false positive, false negative and detection rates are more useful than trust score over time for a single node. The author considers packet forwarding, time synchronization and data manipulation attacks.

4.3.4. Signature Based Designs

Onat and Miri [35] use RSSI and trustee-sourced packet arrival rate to detect intruders in WSNs. The authors use a signature based detection technique auditing data from a

traffic based collection process which considers multitrust data. Onat and Miri theorized that buffer sizes limited by memory constraints would lower false positives, however experimental results did not support this. Their attack model includes spoofing and resource depletion.

Zamani et al. [82] studied an IDS using a signature based detection technique auditing data from a using a traffic based collection process inspired by immunology and danger theory. Molecular patterns (MPs) are the signature analogs in this design. The authors' approach was informed by the distributed nature of a biological immune system. Zamani et al.'s design has two types of IDS actors: stationary agents (thymus, bone marrow, lymph node and local tissue) act like body tissues and mobile agents (B cells, T cells and antigen presenting cells) play the role of immune cells. The authors' detection criteria hinges on costimulation which is the weighted sum of the totals of safe concentration levels, danger concentration levels and density of matching molecular patterns. They report false negative and false positive rates of 40.0 and 8.23%, respectively. Their attack model focuses on DDoS.

4.3.5. Specification Based Designs

Ioannis et al. [83] propose a multitrust IDS with traffic based collection that audits the forwarding behavior of suspects to detect blackhole and greyhole attacks launched by captured nodes based on the the rate (versus the count) of specification violations. Intrusion detectors use majority voting to compensate for slander attacks from malicious nodes and unintentional hidden node collisions. The pro of this study is the identification of a $2:1$ cooperative (voting based) audit period to local (specification based) audit period ratio as the best practice based on the trade between false negative rate and detection latency. Intrusion detectors vote asynchronously; the con of this study is the authors' brief discussion on how to manage vote timing.

4.4. Ad Hoc Networks

We apply the classification tree to organize seven IDS techniques in ad hoc networks and summarize the results in Table 4.

4.4.1. Anomaly Based Designs

Sarafijanović and Le Boudec [84] study an immunology-inspired approach targeted for MANET applications. The authors pursue an unsupervised anomaly-based approach and focus on four concepts: a virtual thymus, clustering, a danger signal and memory detectors. They intend to advance the state of the art by eliminating the training phase used by contemporary semi-supervised anomaly-based approaches, adapting to changes in user profile and reducing the false positive rate that is common in anomaly-based approaches. Sarafijanović and Le Boudec's attack model consider greyhole attacks on user data and DSR protocol. The authors provide three performance metrics: true positive rate, false positive rate and detection latency (s).

Zhang and Lee [37] propose a semi-supervised, distributed, multitrust traffic based IDS. The authors' design audits a generic routing table, but they argue that their approach generalizes to any ad hoc routing, MAC or application layer protocol. Zhang and Lee base their prototype on the RIPPER classifier. The authors weight reported data based on proximity; reported data from a close neighbor is more important than the same data from a distant neighbor. They use majority voting at the system level to clarify low confidence results at the node level. Zhang and Lee govern a key metric (false positive rate) in their design by parameterizing RIPPER so that it results in unclassified data at a rate equal to or below the desired false positive rate. Zhang et al. [85] is an extension of [37] in which they compare RIPPER with SVM Light and report simulation results for AODV, DSDV and DSR environments. SVM Light outperformed RIPPER for AODV and DSR, but the RIPPER and SVM Light results were similar for DSDV. Their attack model focuses on routing attacks.

4.4.2. Reputation Based Designs

Bella et al. [30] propose a behavior based IDS that bases node reputation on the energy it uses for others in comparison with the energy it uses for itself: specifically, the ratio of packets forwarded to packets sourced. They calculate aggregate reputation score as the weighted sum of the locally observed reputation score, the Neighbor Reputation Table (NRT) value, historical global reputation score, the Global Reputation Table (GRT) value and a third party recommendation; the design ages scores such that the reputation of inactive nodes deteriorates. One con of this study is that nodes that do not have a demand for forwarding will be penalized unfairly; also, using reputation score similarity as the key metric is not intuitive. The authors focus on detecting selfish nodes.

Buchegger and Le Boudec [47] propose a distributed IDS called CONFIDANT which extends DSR by measuring reputation with "no forwarding" behavior. The authors distinguish three levels of multitrust: *experienced* data is a firsthand account which has the most weight, *observed* data which has less weight than experienced data happens in the neighborhood (within radio range) and *reported* data which has less weight than experienced or observed data is an account coming from outside the neighborhood. Borrowing from the field of ecology, they classify nodes into one of three categories: suckers (who always assist neighbors), cheats (who never assist neighbors) and grudgers (who assist neighbors until they experience nonreciprocation). One pro of this study is the capability for reformed or falsely detected nodes to rejoin the network. The authors focus on detecting selfish nodes.

Michiardi and Molva [65] propose an IDS called CORE. Neighbors of a suspect calculate its *subjective* reputation score from experience of some property f (for example,

Table 4: Classification of Ad Hoc Network IDSs

	detection technique	collection approach	multi-trust	analysis
Sarafijanović Technique [84]	anomaly	traffic	yes	data mining
Zhang and Lee Technique [37, 85]	anomaly	traffic	yes	data mining
Bella Technique [30]	reputation	behavior	yes	pattern matching
CONFIDANT [47]	reputation	traffic	yes	pattern matching
CORE [65]	reputation	traffic	yes	pattern matching
Vigna Technique [86]	signature	traffic	yes	
Specification Based Monitoring of AODV [87]	specification	traffic	yes	pattern matching

DSR routing or packet forwarding) weighting earlier and later observations differently, and nodes calculate a suspect's *functional* reputation over multiple f weighting various f differently and aging (decreasing over time) the reputations of inactive nodes. In CORE, each node regards every other node as either trusted (positive reputation) or misbehaving (negative reputation); nodes deny service requests and ignore reputation information from misbehaving nodes. Pros of this study are the toleration of slander attacks and distinct sanctions for selfish and malicious nodes. The cons of this study are the dependent variables: number of evaluations used to calculate global reputation and variance of global reputation. The authors focus on detecting selfish nodes.

4.4.3. Signature Based Designs

Vigna et al. [86] propose a multitrust traffic based IDS. The authors focus on auditing AODV data. They instrument a physical experiment; in contrast, most of the literature relies on modeling or simulation results. The authors claim, on aggregate, a 95% detection rate and a 6% false positive rate. They found packet drop attacks had the best detection rate and spoofing attacks had the lowest false positive rate. Vigna et al. consider spoofing, blackhole, resource depletion and routing attacks.

4.4.4. Specification Based Designs

Tseng et al. [87] use an AODV based FSM to establish a specification for a traffic based IDS. Distributed network monitors maintain an FSM for each routing transaction (request and reply). States are normal, alarm or suspicious; in suspicious states, the network monitor asks its peers for additional insight on the transaction. The con of this study is the reliance on a modification of AODV to support their design; specifically, this extended AODV has one additional field, previous node, in each message. The authors consider man in the middle and tunneling attacks.

4.5. Mobile Telephony

We apply the classification tree to organize seven IDS techniques in mobile telephony and summarize the results in Table 5.

4.5.1. Anomaly Based Designs

Hall et al. [20] propose Anomaly Based Intrusion Detection (ABID), a semi-supervised IDS that uses a machine learning technique (Instance Based Learning) and is based on mobility profiles. The authors point out an IDS based on mobility is particularly effective against node capture attacks because the thief will likely have a different movement pattern than the owner. Two controls parameterize their system: precision level (PL) enlarges or constrains the granularity of the location data (digits of precision used from latitude/longitude), and sequence length (SL) extends or reduces the size of tracks under analysis. ABID classifies test data that is too similar to the training data as anomalous in order to counter a profile replay attack. The con of this study is the extremely long training phase: up to six months. The authors focus on replay and node capture attacks.

Li et al. [31] propose a cross layer behavior based IDS using neural networks called Host based Multi-level Behaviour Profiling Mobile IDS (HMBPM). They prosecute application layer features such as URL visited, network layer features such as packets transmitted and machine layer features such as microprocessor load. Li et al. establish three Radial Basis Function neural nets for analysis: one each for call details, device usage and Bluetooth activity; the Multi-Level Behaviour Selector changes the neural net feature set over time as the behavior pattern changes. The con of this study was the error rate which is as high as 36.4%. The authors focus on spoofing and node capture attacks.

Samfat and Molva [19] propose a multitrust IDS called Intrusion Detection Architecture for Mobile Networks (IDAMN) that runs in real-time (it can detect an intruder while a call is in progress) and distributes computation hierarchically. The authors minimize the amount of profile data which enhances privacy and prevents profile replay attacks. IDAMN uses three techniques to detect intrusions: studying user velocity to detect clones, looking for dispar-

Table 5: Classification of Mobile Telephony IDSs

	detection technique	collection approach	multi-trust	analysis
ABID [20]	anomaly	traffic		data mining
HMBPM [31]	anomaly	behavior		data mining
IDAMN [19]	anomaly	traffic	yes	both
BBID [88]	signature	behavior		pattern matching
ESM [89]	signature	behavior		pattern matching
Gibraltar [90]	signature	behavior	yes	pattern matching
MABIDS [91]	signature	behavior	yes	pattern matching

ity between switch/base station activity and user density and comparing user behavior with user profile. IDAMN user profiles have three components: mobility/itinerary, call details and speech. For the call details component of the user profile, IDAMN weights recent data more heavily than older data. For the mobility component of the user profile, IDAMN weights frequent itineraries more heavily than rare itineraries. The pro of this study is the false positive rate which ranges from 1 to 7%. The con of this study is the detection rate which is as low as 60%. These results are counterintuitive: generally, anomaly detection techniques have weak false positive rates and excellent detection rates. The authors focus on spoofing and node capture attacks.

4.5.2. Signature Based Designs

Jacoby et al. [88] propose a collection approach called Battery Based Intrusion Detection (BBID) and a detection technique called Host Analysis Signature Trace Engine (HASTE). The authors argue that behavior based collection is the best fit for resource constrained applications, such as mobile telephony handsets. The attack model of Jacoby et al. is specific; they detect attackers who prevent the target device from entering a lower Advanced Power Management (APM) power state in order to exhaust its energy prematurely. The authors concede that these attacks can be detected by other means, but the detection latency is unacceptable. As a clarification, they refer to their signature based approach as "rule based anomaly detection." BBID analyzes power consumption in each state and the transition pattern between states. One pro of this study is the accommodation of differences in battery technologies (for example, Li-ion versus NiMH) and operating conditions (for example, temperature). The con of this study, which the authors point out, is that BBID itself will affect the power consumption of a handset and therefore has the possibility to interfere with its results.

Martin et al. [89] propose an IDS called Power Secure Architecture (PSA) to guard against their novel attack model: attackers who exhaust the target battery prematurely via service request, benign and malignant power attacks. PSA combines resource management with an intrusion detection design called Energy Signature Monitor. As a clarification, they refer to expected or normal behavior as a signature. Martin et al. associate a power signature with each process that runs on the target. One con of this study is a lack of numerical results. Another con of this study is a questionable threat model; the authors treat an animated GIF served by a web page as an attack.

Castle et al. [90] propose an IDS called Gibraltar that builds upon the prior work in [88]. Prior to going online, the authors created signatures for several forms of attack by profiling the battery current. Gibraltar includes a static, reactive response component that collects additional audit data [process, network and (Windows) registry activity] for forensic use. One pro of this study is the tiered dictionary which is distributed across handsets and servers. The authors focus on DoS and LSASS attacks.

Kannadiga et al. [91] propose an IDS called Mobile Agent Based IDS (MABIDS). This design comprises transient thick mobile agents (MAs) on fixed infrastructure nodes, transient thin MAs on mobile nodes and a mobile agent server (MAS). Thick MAs perform collection and analysis functions while thin MAs only perform collection; the MAS performs the related analysis in the latter case. The MAS dispatches thick MAs to fixed infrastructure nodes when they may be under attack and thin MAs to mobile nodes on a periodic basis. The design rationale is to take advantage of the power of the fixed infrastructure nodes, leverage the rich data set present on nodes when under attack and conserve resources of the mobile nodes. To clarify, the authors use the term "remote" to refer to mobile nodes and "mobile" to refer to the transient agents the MAS may dispatch to both fixed and mobile nodes. One con of this study is a lack of numerical results. The authors say their design is relevant to DoS, buffer overflow and doorknob rattling attacks.

4.6. WMNs

We apply the classification tree to organize four IDS technique in WMNs and summarize the results in Table 6.

4.6.1. Anomaly Based Designs

Wang et al. [92] propose a cross layer detection technique that pursues data from the physical, link and net-

Table 6: Classification of WMN IDSs

	detection technique	collection approach	multi-trust	analysis
Cross-layer Based IDS [92]	anomaly	traffic		data mining
HPT [66]	anomaly + signature	traffic	yes	
Li Technique [93]	specification	traffic	yes	pattern matching
Probability Based IDS [94]	specification	traffic	yes	pattern matching

work layers of the stack. The specific machine learning technique (Bayesian network, decision tree or SVM) is a control variable in the experiment. The pros of this study are excellent detection and false alarm rates for different attacks for their cross layer design compared to a single (network) layer design. Their attack model considers probe flooding, blackhole and greyhole attacks.

4.6.2. Anomaly + Signature Based Designs

Yang et al. [66] study a hierarchical and proxy based (contrast with behavior based) IDS approach called Hierarchical Proxy based Topology (HPT). Their main contribution deals with a multitrust framework: Each neighborhood within the WMN has a proxy that collects and analyzes audit data. If the local proxy cannot determine if a node is an intruder or not, it escalates the audit to the central console which may request input from other local proxies. One con of this study is a lack of numerical results. The authors do not tie their IDS to any attack type.

4.6.3. Specification Based Designs

Li et al. [93] propose a multitrust IDS that uses a specification based design that checks for contention window conformance; following a collision, intruders do not stand down for as long as they should. IDS roles are based on the WMN role; gateways, mesh routers and mesh clients perform different IDS functions and respond differently to detections. The con of this study is the weak attack model which only considers selfish adversaries. The authors focus on detecting selfish nodes.

Zhou et al. [94] study a traffic based collection approach using 802.16 (WiMAX) mesh network administration messages: Mesh Network Configuration (MSH-NCFG), Mesh Network Entry (MSH-NENT), Mesh Distributed Scheduling (MSH-DSCH), Mesh Centralized Scheduling (MSH-CSCH) and Mesh Centralized Configuration (MSH-CSCF). Multitrust data plays a key part in their design: it compares the communication state a node reports for itself with the state other nodes report for it. Less similarity indicates a higher probability of attack. The communication state consists of base station and subscriber station visibility; the authors extract this state from the mesh network administration messages. One con of this study is a lack of numerical results. The authors focus on sinkhole and wormhole attacks.

4.7. CPSs

We apply the classification tree to organize four IDS techniques in CPSs and summarize the results in Table 7.

4.7.1. Anomaly Based Designs

Tsang and Kwong [95] propose a multitrust IDS called Multi-agent System (MAS). Their analysis function, Ant Colony Clustering Model (ACCM), is biologically inspired by its namesake, the ant colony. The authors intend for ACCM to reduce the characteristically high false positive rate of anomaly based approaches while minimizing the training period by using an unsupervised approach to machine learning. MAS is hierarchical and contains a large number of roles: monitor agents collection audit data, decision agents perform analysis, action agents effect responses, coordination agents manage multitrust communication, user interface agents interact with human operators and registration agents manage agent appearance and disappearance. Tsang and Kwong's results indicate ACCM slightly outperforms the detection rates and significantly outperforms the false positive rates of k-means and expectation-maximization approaches. One pro of this study is that it uses a standard data set, KDD Cup 1999, for testing. Another pro of this study are the great false positive results: the ACCM false positive rate peaks at 6%. The authors focus on zero-day (unknown) attacks: specifically, the KDD Cup 1999 data set.

The IDS in [61, 62, 63] that relies on voting is one example of using anomaly detection results in the context of multitrust. One con of this study is the lack of simulation to validate the probability model. The authors consider data manipulation and spoofing attacks.

4.7.2. Anomaly + Signature Based Designs

Porras and Neumann [41] study a hierarchical multitrust behavior based IDS called Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) using complementary signature based and

Table 7: Classification of CPS IDSs

	detection technique	collection approach	multi-trust	analysis
ACCM/MAS [95]	anomaly	behavior + traffic	yes	data mining
HPMIDCPS [61, 62, 63]	anomaly	traffic	yes	pattern matching
EMERALD [41]	anomaly + signature	behavior	yes	pattern matching
Shin Technique [12]	anomaly + signature	traffic	yes	

anomaly based analysis. The authors identify a signature based analysis trade between the state space created/runtime burden imposed by rich rule sets and the increased false negatives that stem from a less expressive rule set. Porras and Neumann highlight two specific anomaly based techniques using statistical analysis: one studies user sessions (to detect live intruders), and the other studies the runtime behavior of programs (to detect malicious code). EMERALD provides a generic analysis framework that is flexible enough to allow anomaly detectors to run with different scopes of multitrust data (service, domain or enterprise). One con of this study is a lack of numerical results. The authors do not tie their IDS to any attack type.

Shin et al. [12] present an extension of an existing WSN technique using one hop clustering; in a one hop cluster every member falls within radio range of the cluster head. They combine one hop clustering for effective intrusion detection (the "second" clustering) with multi hop clustering for efficient data aggregation (the "first" clustering) into a hierarchical two level clustering approach to strike a balance between security and efficiency. This results in a four layer hierarchy: member nodes (MN) are the leaves, cluster heads (CH) manage MNs, gateways bundle clusters and a base station is the root of the hierarchy. These different roles analyze audit data the same way, but they respond differently. This heterogeneous approach has the advantage of minimizing the question of trustworthiness; the CHs need to establish trust while the MNs do not. They demonstrate that one hop clustering is particularly effective when detecting spoofing attacks. One pro of this study is the numerical results; the authors report detection rates for jamming, spoofing, hello flooding, data manipulation, greyhole, eavesdropping, routing and sinkhole attacks. One con of this study is the results are conflicting; for example, they claim a 25 - 43% detection rate for spoofing attacks in a table summarizing average detection rate and a 60 - 100% detection rate for spoofing attacks in a figure that plots average detection rate as a function of hop counts.

4.8. Others

We apply the classification tree to organize 15 IDS techniques not specifically designed for WLANs, WPANs, WSNs, ad hoc networks, mobile telephony, WMNs or CPSs and summarize the results in Table 8.

4.8.1. Anomaly Based Designs

Stibor et al. [71] perform immunology-inspired IDS research. The authors examine the DCA from a mathematical perspective and its applicability to anomaly detection. They claim its parallelism limits its utility in this domain and base their analysis on the deterministic variant of the DCA. Stibor et al. show how to represent the signal processing element of the DCA as a set of linear classifiers. The authors do not anchor their study to a single brand of wireless network or provide performance data.

Farid and Rahman [21] investigate a semi-supervised approach to the analysis function of a traffic based IDS. They extend the naive Bayesian algorithm into their Improved Adaptive Bayesian Algorithm (IABA). The key innovation of IABA is a feedback loop allowing the model to learn from misclassified test data; learning amounts to changing attribute weights. The pros of this study are demonstrated improvements in training times, testing times, false positives and false negatives. The authors focus on zero-day (unknown) attacks: specifically, the KDD Cup 1999 data set.

Jones and Li [24] study an IDS using behavior based collection that applies statistical analysis to timing enriched system call sequences by extending the work of Hofmeyr et al. in [99] and Lee and Stolfo in [100]. In the training phase, their design identifies all k length system call sequences in a set of normal training data and includes the time interval between calls and calculates a mean and standard deviation vector over the time intervals for each cluster, (each instance of a sequence is a *case* and the collection of all cases for a sequence is a *cluster*) applies three filters to the data set to *qualify* it and (they calculate a z-score for each case and discards cases (rows) above z_a, ignore time intervals (columns) with a normalized standard deviation that is above C_s and remove clusters where less than T_v of cases pass the first filter) calculates the fraction of usable cases in the training data, P_v. In the testing phase they repeat this procedure on a suspect session (P_v is retitled P_m in this phase); if $P_m \ll P_v$, then their design detects an intrusion. The con of this study is a lack of numerical results: externally valid metrics like aggregate false positive, false negative and detection rates are more useful than z, P_v and P_m scores. The authors focus on shellcode attacks.

Table 8: Classification of Generic Wireless Network IDSs

	detection technique	collection approach	multi-trust	analysis
Deterministic DCA [71]	anomaly			data mining
IABA [21]	anomaly	traffic		data mining
Jones Technique [24]	anomaly	behavior		pattern matching
Snort [96]	combined	traffic		
OSSEC [64]	signature	behavior	yes	pattern matching
Signature Apriori [23]	signature	traffic		combined
Ying Technique [43]	combined	behavior		combined
CSM [40]	signature	behavior	yes	pattern matching
BMSL [97]	specification	combined		pattern matching
SAD [98]	specification	traffic		pattern matching
DPEM [28]	specification	behavior		pattern matching
ADEPTS [27]	combined		yes	
IDAM&IRS [67]	combined		yes	
XIDR [22]	combined	combined	yes	pattern matching
AHA/AAIRS [68]	combined		yes	

4.8.2. Signature Based Designs

OSSEC is a free and open source behavior based IDS implementation [64]. Many recent behavior based techniques extend it by transforming signatures into an OSSEC rule set. OSSEC supports multitrust by incorporating remote "agents" into their framework. The pro of this work is that it provides an open vehicle to apply signature based IDS innovations. The authors do not tie their IDS to any attack type.

Han et al. [23] investigate an IDS using traffic based collection that applies data mining to the distribution and content of network traffic. The authors focus on attack dictionary generation based on deep packet inspection and call their innovation for this capability Signature Apriori. The pro of this work is the experimental design; the authors empirically study Signature Apriori using three real world attack techniques (glacier, IIS unicode exploit and IPHacker).

White et al. [40] investigate dynamic response measures targeted for large networks using Cooperating Security Managers (CSM), a system of behavior based IDSs that cooperate in a decentralized fashion. CSM correlates results from multiple sources (associates them with a single attack). White et al. identify a spectrum of intrusion responses ranging from low impact responses that are appropriate for weak or low probability attacks to high impact responses that are appropriate for severe or high probability attacks. One con of this study is the requirement to run trusted software on a suspect node; another con of this study is the alerting of the node originating the suspicious behavior which gives the adversary the opportunity to reduce aggression while still causing damage. The authors do not tie their IDS to any attack type but talk through a doorknob rattling attack as an example.

4.8.3. Specification Based Designs

Uppuluri and Sekar [97] propose a means and a methodology for specifying a system called Behavioral Monitoring Specification Language (BMSL), which specifies both normal and abnormal behaviors for an IDS using traffic and behavior collection; BMSL models the event details and event sequencing. The authors' IDS transforms BMSL programs into detection engines (DEs). The methodology of Uppuluri and Sekar begins with specifying generic system behaviors, then focuses on highly privileged functions, then specifies application specific behaviors, then tailors the specification for each installation and ends by specifying misuse signatures. They combine the BMSL approach to specification based IDS with a signature based IDS in order to match the detection rate of a signature based IDS. The pro of this study is a 100% detection rate. One con of this study is the requirement to store and update a large attack dictionary which eliminates one of the benefits of specification over signature based designs. Another con of this study, which the authors acknowledge, is that BMSL does not effectively model time; for example, benign user error may account for one failed authentication in one day while ten failed authentications in a minute may indicate an adversary trying to crack the authentication. The authors focus on detecting attacks present in the 1999 DARPA/AFRL and 1999 DARPA/Lincoln Labs data sets.

Sekar et al. [98] use extended finite state automata (EFSAs) to establish a specification for a traffic based IDS. They combine the EFSA approach to intrusion detection with an anomaly based IDS that uses unsupervised machine learning. The con of this study is requiring the IDS to run a processor and core memory intensive machine learning module which eliminates one of the ben-

efits of specification over anomaly based designs. The authors focus on detecting attacks present in the 1999 DARPA/Lincoln Labs data set.

Ko et al. [28] propose Distributed Program Execution Monitor (DPEM) which uses the Parallel Environment Grammars (PE-grammars) language for an IDS using behavior collection. The con of this study is a lack of numerical results: externally valid metrics like aggregate false positive, false negative and detection rates would be useful in addition to detection latency. The authors focus on attacks on rdist, sendmail and binmail UNIX programs.

4.8.4. Combined Designs

Snort is a free and open source traffic based IDS implementation [96]. Many recent traffic based collection techniques extend it by transforming signatures into a Snort rule set. The authors claim that Snort can operate as an anomaly based or a signature based IDS. The pro of this work is that it provides an open vehicle to apply anomaly or signature based IDS innovations. The authors do not tie their IDS to any attack type.

Ying et al. [43] propose a behavior based IDS that combines log file analysis with neural network backpropagation. This is a combined approach with a log file analyzer, which must be initialized with a rule set, detecting signatures and a semi-supervised neural network detecting anomalies. The con of this study, which the authors point out, is an extensive training period which can span weeks. The authors do not tie their IDS to any attack type.

Svecs et al. [22] present an IDS called Cross-layer Intrusion Detection and Response (XIDR). XIDR combines both detection techniques (anomaly and signature based) and collection approaches (behavior and traffic based) and use both local and global intrusion responses. XIDR measures user history (by noting positive events like successful authentication or negative events like failed authentication, probative actions and previous alerts), confidence of intrusion detection (giving more confidence to detections stemming from more specific rules) and the cost of intrusion response (assigning greater cost to lower layer responses); it uses these to choose an intrusion response. Their results suggest that cross layer detection and response is particularly effective when history (a table associating IP addresses with security related events) informs the decision making. The con of this study is a nonintuitive metric: false negative, false positive or detection rates would be more clear than $1 - \text{XIDR performance/single layer performance}$. The authors focus on SQL injection attacks.

Mu et al. [67] study the response function using Intrusion Detection Alert Management and Intrusion Response System (IDAM&IRS). The authors identify and create a taxonomy for 15 response factors which serve as input to intrusion response functions. They identify two components to intrusion response: response start time (as opposed to response duration time) and response measure; they propose that different response factors should inform each of these two components. This paper claims that contemporary response functions disregard negative impacts on the network (effect on legitimate users) and only consider positive impacts (effect on intruders). The con of this study is a lack of any numerical results. The authors do not tie their IDS to any attack type.

Foo et al. [27] investigate the response function by focusing on attack containment and tolerance using Adaptive Intrusion Tolerant System (ADEPTS) which extends [67]. Negative impact on the system, detection confidence and threat level (the ratio of false negatives to false positives) inform the response function. The authors present Portable I-graph Generation that transforms a system services description (SNet) and set of vulnerability descriptions into modified fault trees which identify opportunities for containment. Each node in the I-graph is the goal of some attack and has a compromised confidence index (CCI) score which indicates the probability of compromise. They measure ADEPTS by the fraction of system functions available during an attack; disruption caused by response measures and successful attacks decrease this survivability score. When computing candidate response measures, ADEPTS uses the SNet edge types leading to the endangered node and response index. Response index compares the effectiveness and disruptiveness of the response measure. ADEPTS decreases the effectiveness index for a measure if it continues to receive alerts for an intruder and increases the effectiveness index for a measure if it runs to completion. The pro of this study is a rich attack model. One con of this study is the CCI calculation which departs from established probability techniques. Another con of this study is the strong assumption that truth data is available at runtime to determine false positives and negatives. The authors consider DoS, data manipulation and exfiltration attacks.

Ragsdale et al. [68] study adaptive analysis and response functions using Adaptive Hierarchical Agent based IDS (AHA) and Adaptive Agent based Intrusion Response System (AAIRS). In AHA, management agents tune analysis by running different quantities of tool agents based on threat level, different types of tool agents based on attack vector and changing the confidence associated with the detection results based on false positives and false negatives. Their response function contains a feedback loop governed by the effectiveness of previous responses and detection confidence (false positives over true positives). AAIRS improves on contemporary designs by basing intrusion responses not only on the type of attack but also the specific parameters of the attack [67]. The con of this study, like Foo et al. [27], is the strong assumption that truth data is available at runtime to determine false positives, false negatives and detections. The authors do not tie their IDS to any attack type.

5. Lessons Learned

In this section, we discuss the commonality and variability of IDS techniques as applying to various wireless systems and report lessons learned. We first discuss the pros and cons of IDS techniques and thus their suitability of applying to various wireless systems. Then, we discuss the most and least studied IDS techniques in the literature based on our survey. Lastly, we identify gaps yet to be explored and revisit IDS techniques that deserve further research for certain wireless systems.

Tables 9 and 10 summarize the pros and cons of IDS techniques, respectively, as applying to various wireless systems. Table 11 identifies the most and the least researched IDS techniques. That is, which IDS techniques have been researched the most or the least in a given wireless system. These tables use the target system dimension to aggregate the survey results from Section 4.

5.1. Pros and Cons of IDS Techniques as Applying to Wireless Systems

Here we discuss the suitability of IDS techniques in terms of their pros and cons when applying to various wireless systems. Refer to Tables 9 and 10.

Signature based approaches, because of their minimal processing burden, avoidance of empirical training data can benefit WPANs and mobile telephony (specifically handsets); these applications have limited processing capabilities, lack a well defined concept of operations and can easily update attack dictionaries. Also, because of their minimal processing burden, signature based approaches can benefit WSNs and CPSs (specifically RTUs) which have limited processing capabilities.

Mobile telephony and CPSs, because they have well defined concept of operations where anomalies will sharply contrast baseline behavior, can benefit from anomaly based approaches. Also, anomaly based approaches, because of their strength in detecting unknown attacks, can benefit WLANs, WPANs and ad hoc networks which have a lot of untrusted actors. WSNs can benefit from anomaly based approaches because of their minimal nonvolatile storage requirement; an anomaly based approach does not require an attack dictionary.

WSNs and CPSs, which have well defined concepts of operation from which humans can extract invariant conditions, can benefit from specification based approaches.

Reputation based approaches can benefit all systems in finding selfish nodes. They will especially benefit applications for which selfish nodes are considered intolerable and a sanctioning policy on selfish nodes is well defined.

Behavior based approaches, because they can exploit their consistent behavior, can benefit WSNs and CPSs which have well defined concepts of operation. While WLANs, WPANs, ad hoc networks, mobile telephony and WMNs do not have this property, they can benefit from behavior based approaches because of their minimal memory burden; the alternative, a traffic based approach, requires a lot of storage.

Traffic based approaches can benefit WSNs, WMNs and CPSs which are typically stationary because the lack of mobility will eliminate one source of error in the data set. Specifically, data sets will not have artifacts caused by changes in distance, multipath reflections or obstructions. While WLANs, WPANs, ad hoc networks and mobile telephony are more mobile, they can benefit from traffic based approaches because their data sets are rich with features unavailable to wireline applications such as RSSI and SNR.

Multitrust based approaches can benefit WMNs which have a stable set of neighbors and strong trust relationships; this enhances the credibility of multitrust data. Also, multitrust based approaches can benefit WSNs and CPSs which at least have a stable set of neighbors. While WLAN, WPAN, ad hoc network and mobile telephony populations are more dynamic, they can benefit from multitrust based approaches because a data set expanded by multitrust provides a fuller picture of the system even if that data set is biased by untrusted inputs [59]. They key problem in this case is weighting trusted data more heavily than untrusted data.

Because they cannot store a large attack dictionary, WPAN, WSN, and mobile telephony (especially handset) applications present a challenge for signature based approaches. While they can accommodate a large attack dictionary, ad hoc network, WMN and CPS applications will struggle to keep the attack dictionaries fresh for signature based approaches.

Because of potential revenue loss in mobile telephony and the sanctioning of life-critical nodes in CPS applications, anomaly based approaches present a challenge because of their high false positive rates. Although they are free of financial and life-critical concerns, WLAN, WPAN and ad hoc network applications lack a well defined concept of operations and anomalies will not sharply contrast baseline behavior. Finally, WSN and WMN applications will struggle to manage the high false positive rates of anomaly based approaches.

WLAN, WPAN, ad hoc network, mobile telephony and WMN applications present a challenge for specification based approaches because an expert will struggle to distill a specification for applications without well defined use cases. Although they do have well defined use cases, specification based approaches still require a costly expert analysis to produce a specification for WSN and CPS applications.

Because of potential revenue loss in mobile telephony and the sanctioning of life-critical nodes in CPS applications, reputation based approaches present a challenge because they target selfish nodes rather than bad nodes. A mobile telephony operator still generates revenue from selfish nodes and a CPS needs selfish nodes for continuity of operation. Although they are free of financial and life-critical concerns, WLAN, WPAN, WSN, ad hoc network and WMN applications will still struggle to manage the

Table 9: Pros of IDS Techniques For Wireless Networks

	WLANs	WPANs	WSNs	ad hoc networks	mobile telephony	WMNs	CPSs
signature based	variable CONOP, easy updates	variable CONOP, constrained resources	minimal processing burden	high detection rate	variable CONOP, constrained resources, easy updates	high detection rate	minimal processing burden
anomaly based	unknown attacks	unknown attacks	minimal persistent storage	unknown attacks	well defined CONOP	well defined CONOP	well defined CONOP
specification based	unknown attacks	unknown attacks	well defined operation	unknown attacks	unknown attacks	unknown attacks	well defined operation
reputation based	find selfish actors	find selfish actors	find selfish actors	find selfish actors	find selfish actors	find selfish actors	find selfish actors
behavior based	low false negatives	minimal memory	low false negatives	minimal memory	minimal memory	minimal memory	low false negatives
traffic based	metadata rich	metadata rich	less data set error	metadata rich	metadata rich	less data set error	less data set error
multitrust	expanded data set	expanded data set	credible data set	expanded data set	expanded data set	credible data set	credible data set

Table 10: Cons of IDS Techniques For Wireless Networks

	WLANs	WPANs	WSNs	ad hoc networks	mobile telephony	WMNs	CPSs
signature based	dictionary freshness	dictionary size	dictionary size and freshness	dictionary freshness	dictionary size	dictionary freshness	dictionary freshness
anomaly based	variable CONOP	variable CONOP	high false positive	variable CONOP	revenue impact	high false positive	reliability impact
specification based	lack common use cases	lack common use cases	costly expert analysis	lack common use cases	lack common use cases	lack common use use cases	costly expert analysis
reputation based	selfish actor sanctions	selfish actor sanctions	selfish actor sanctions	selfish actor sanctions	revenue impact	selfish actor sanctions	reliability impact
behavior based	erratic profiles	erratic profiles	dormant attacker	erratic profiles	erratic profiles	erratic profiles	dormant attacker
traffic based	inconsistent visibility	limited storage	limited storage	inconsistent visibility	limited storage	inconsistent visibility	inconsistent visibility
multitrust	dynamic population	dynamic population	increased storage burden	dynamic population	dynamic population	increased storage burden	federated population

sanctioning of good but selfish nodes.

Because their profiles are unpredictable, WLAN, WPAN, ad hoc network, mobile telephony and WMN applications present a challenge for behavior based approaches. Although they have predictable behaviors, WSN and CPS applications will still struggle with behavior based approaches when facing a dormant attacker. An effective attacker does not necessarily attack the target system immediately: An opportunistic attacker lies in wait until the environment favors his cause, and an insidious attacker remains dormant until his force reaches a critical mass inside the target's domain [101].

Because of their limited storage, especially WPAN, WSN and mobile telephony (especially handset) applications present a challenge for traffic based approaches. Although they have more substantial storage, ad hoc network, WMN and CPS applications will still struggle with traffic based approaches using multitrust because different positions will have different visibility.

Because their dynamic populations make it difficult to form trust relationships, WLAN, WPAN, ad hoc network and mobile telephony applications present a challenge for multitrust based approaches. Also, their federated populations cause the same difficulty for CPS applications. Although their populations are more stable and managed unilaterally, WSN and WMN applications will still struggle with multitrust based approaches due to increased storage burden.

5.2. Most Studied IDS Techniques in the Literature

We summarize the most and least studied IDS techniques in Table 11. Topics with no research are marked with cyan, those with little research are marked with grey and topics with significant research are marked with red. Further, each topic is filled with a number quantifying exactly the number of existing works cited on the topic, with $\times$ indicating that it deserves research attention.

We mark the most studied IDS techniques as applied to various systems with red in Table 11. Specifically, signature based techniques applied to WLANs, WSNs and mobile telephony, anomaly based techniques applied to WLANs, WSNs, mobile telephony and CPSs, specification based techniques applied to WMNs, reputation based techniques applied to WSNs and ad hoc networks, behavior based collection techniques applied to mobile telephony, traffic based collection techniques applied to WLANs, WSNs, ad hoc networks, mobile telephony, WMNs and CPSs and multitrust techniques applied to WLANs, WSNs, ad hoc networks, mobile telephony, WMNs and CPSs are well studied.

In general, these correspond with high efficacy applications we identified in Sections 3.2.5, 3.3.3, 3.4.3 and 3.5.4.

5.3. Least Studied IDS Techniques in the Literature

Table 11 indicates there is no research (marked with cyan) in IDS techniques as applied to various wireless systems. Specifically, there is no research with regard to signature based techniques applied to WMNs and CPSs, specification based techniques applied to WLANs, WPANs, mobile telephony and CPSs, reputation based techniques applied to WLANs, WPANs, mobile telephony, WMNs and CPSs and behavior based techniques applied to WLANs, WPANs and WMNs.

Table 11 indicates there is little research (marked with grey) in IDS techniques as applied to various wireless systems. Specifically, there is little research with regard to signature based techniques applied to ad hoc networks, anomaly based techniques applied to ad hoc networks and WMNs, specification based techniques applied to WSNs and ad hoc networks and behavior based techniques applied to WSNs, ad hoc networks and CPSs.

In general, these correspond with low efficacy applications we identified in Sections 3.2.5, 3.3.3, 3.4.3 and 3.5.4.

5.4. Revisiting IDS Techniques and Gaps in IDS Research

From Tables 9, 10 and 11 we identified several gaps in the literature. Many of these gaps do not need investigative attention, but some do.

Few have applied signature based designs to ad hoc networks, and none have applied them to WMNs or CPSs. The inability to detect unknown attacks and the need to store and update a large attack dictionary makes signature based designs unsuitable for these target systems.

Few have applied anomaly based designs to ad hoc networks and WMNs. Anomaly based designs' large false positive rates and the transient populations of ad hoc networks make these ineffective combinations.

None have applied specification based designs to WLANs, WPANs, mobile telephony or CPSs while only a few have applied them to WSNs and ad hoc networks. WLANs, WPANs and mobile telephony networks lack a single encompassing concept of operation which make specification based designs ineffective. Researchers should pursue specification based designs for CPSs because they are particularly applicable to CPSs which have well-defined operations. Signature based approaches are not workable because of maintenance difficulty, and reputation management based approaches are not workable because of federation. The false alarm rates for specification based designs are better than anomaly based designs, and the well defined use cases for CPSs yield a rich set of phenomena to specify.

None have applied reputation management based designs to WLANs, WPANs, mobile telephony, WMNs or CPSs. Because their tightly specified communication infrastructure may not be able to handle the associated gossip, reputation management based designs are not suitable for mobile telephony or CPSs. Because their populations are relatively static, the overhead of computing trust will not trade favorably with the benefit of using historical audit data. Nevertheless, researchers should pursue reputation management based designs for WLANs, WPANs and WMNs.

Table 11: Most and Least Studied IDS Techniques (cyan: no research, grey: little research, red: significant research, ×: deserving more research)

	WLANs	WPANs	WSNs	ad hoc networks	mobile telephony	WMNs	CPSs
signature based	4	2	4	1	4	1	2
anomaly based	5	2	7	2	3	2	4
specification based			1	1		2	×
reputation based	×		4	3		×	
behavior based	×1	1	2	1	5		2
traffic based	6	3	9	6	2	4	3
multitrust	2	1	6	7	3	3	4

There are research gaps for behavior based approaches applied to WLANs, WPANs and WMNs, and researchers should pursue behavior based approaches for them.

Summarizing above, we mark × in Table 11 for IDS techniques which are relatively unexplored in the literature but deserve further research attention, as they have been identified as suitable as well as potentially impactful for the respective wireless systems identified. When considering the application domain in particular, Table 11 reveals that WLANs, WPANs, WMNs and CPSs suffer from a lack of research on applied IDS with three unrepresented categories.

In addition to the research gaps identified by Table 11, the literature needs studies which provide results in the form of externally valid metrics. Many do not provide numerical results in any form [102, 103, 104, 105, 106, 107, 108, 109, 110].

Furthermore, researchers should gather these measurements for different attack types. For example, one IDS's blackhole attacker detection rate cannot be compared against another IDS's replay attacker detection rate.

When numerical results are reported at all, only detection rate, false positive rate and false negative rate are given usually. For example, detection latency is a critical metric that researchers rarely report on. A 100% detection rate is a great achievement, but if this IDS takes an hour to detect intruders, the adversary may still have enough time to damage the target system.

6. Future Research Areas

Based on our surevy and lessons learned, below we identify several future research areas with suggestions for ways to conduct research in these areas.

1. **Repurpose Existing Work:** A potential research area is to investigate applicability of IDS techniques that, based on our survey, have not been applied to certain systems. These IDS techniques are marked with × in Table 11 for the corresponding wireless systems identified. A possible research direction is to adapt an existing research product to a new target system. As an example, we may apply a response selection algorithm from [22, 27, 40, 41, 67] to WMNs, WSNs, ad hoc networks, WLANs or WPANs. Also, another area is to investigate new IDS techniques that improve upon performance of existing ones. Only contemporary studies that provide clear numerical results enable this line of pursuit. These new IDS techniques may require new detection techniques or a new classification dimension.
2. **Multitrust**: Utilizing multitrust for intrusion detection is relatively unexplored in wireless IDS research but deserves more attention because it increases the dataset available to an IDS. Our survey results indicate that multitust-based intrusion detection for WLANs and WMNs especially deserves more research attention. Multitrust is the concept of using reported information (data from witnesses or third parties). Hearsay or gossip may also be used to refer to reported data. The key problem is guaranteeing the larger data set yields a net gain in key metrics despite the presence of bad-mouthing and ballot stuffing attacks. A preliminary work reported in [52] may shed some light on how to apply multitrust to intrusion detection.
3. **Specification Based Design for CPSs:** Another potential research area is an IDS with a specification based design applied to CPSs. Our survey results confirm specification based designs in general and CPS applications in particular are unexplored. The critical challenge in specification-based designs is to transform a sophisticated system into a formal model. With their well defined actors and functions, CPSs provide an ideal starting point for serious investigation of specification-based designs. Two possible research directions are to create a tool or methodology to transform a system into a formal model and to establish a language or schema for expressing the formal model. These results could feed a CPS analytical model for performance and sur-

vivability analysis. Growing cyber warfare concerns [111] and escalation of cyber warfare rhetoric at the state level [112] make intrusion detection for CPSs an immediately important research area.

4. **Intrusion Response and Repair:** Intrusion response and repair strategies are also relatively unexplored. Possible intrusion responses include evicting individual compromised nodes, isolating compromised segments (microgrid or larger scope) and adjusting detection strength. For example, the IDS can perform better if it adjusts the detection rate based on the type and strength of adversary it faces. Possible repair strategies are to identify compromised segments and for each one: stop operating, revert all nodes to certified software loads and configurations, rekey/reset passwords and progressively resume operation from the production side of the network towards the consumers. Analysis techniques that provide early warning of attacks are another potential research area. These techniques would serve as an enabler by providing a trigger for pre-detection responses. Another research direction is to distinguish early warnings from detections by using the confidence level that accompanies existing analysis techniques.
5. **Metrics:** More research is needed to define wireless IDS performance metrics. When numerical results are reported at all, only detection rate, false negative rate and false positive rate are given usually. However, detection latency is a critical metric that researchers rarely report on. A 100% detection rate is a great achievement, but if this IDS takes an hour to detect intruders, the adversary may still have enough time to damage the target system. We have not found detection latency being studied in the literature, but it is clearly a critical metric. Therefore, researchers should develop detection latency as a key IDS metric. Another new metric could be mitigation latency, which represents the delay between detection and attack repulsion.
6. **Application Layer Data Auditing:** Another research area is to focus on application layer data auditing. The audit of lower layer data that is common to any application has been well-studied, so adversaries expect these defensive measures. A cunning adversary will craft his attack to appear normal in every way possible to avoid widely deployed IDSs. IDSs that audit application layer data focus on detecting the adversary where he must reveal himself to attack the system. A preliminary work can be found in [113, 114] with respect to application layer data auditing for unmanned air vehicles (UAVs) and smart grid cyber physical systems. More effort is needed to investigate the use of threshold monitoring techniques coupled with intrusion detection. Existing works [101, 115] use a binary failure threshold to classify a node as malicious or normal, i.e., a node is considered compromised if it deviates from good behavior once. Other failure threshold criteria based on fuzzy failure criteria [116, 117, 118] may prove to be more effective against environment noises and/or smart attackers.
7. **Modeling and Analysis Methodology:** Model-based analysis techniques such as [61, 62, 63, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134] need to be developed and validated to analyze performance of wireless IDS protocols, identify optimal wireless IDS protocol settings to maximize wireless IDS performance based on performance metrics defined, evaluate further innovation in IDS design and analyze the impact of intrusion detection on system performance and survivability. Configuration items (e.g., number of intrusion detectors, audit interval and detection threshold) impact the detection and false positive rates of the IDS and longevity of the wireless system as a whole. Researchers should identify parameters that have a local maximum and parameters that are covariant. They should establish heuristics for finding the optimal value for the former set and equations that characterize the tradeoff for the latter set.
8. **Adversary Modeling and Countermeasure Design:** Not all adversaries behave the same, so researchers should deepen the complexity of attacker models. The literature is thin on adversary modeling. A preliminary investigation can be found in [63] which characterizes attacker behaviors by reckless, random, and insidious, as well as in [135] which classifes attacker behaviors and devises responses toward these attacker behaviors to maximize the system lifetime. This is not a complete set. The identification of current attacker behavior and/or capture strength is still an unsolved problem and is itself challenging. For example, an oracle attacker could adjust the attacker strength depending on the detection strength to maximize security failure. For countering adversary behavior, more work is called for to apply control theory to design a general control function such that the system can dynamically adjust detection strength in response to attacker strength detected at runtime.
9. **Biology, Immunology and Self-awareness:** A potential research area is to pursue IDS approaches inspired by biology, immunology and self-awareness like [34, 69, 70, 71, 76, 82, 84, 95, 136]. We included nine current references to these techniques in this survey, but many more exist. In particular, they aid detection of unknown attacks; finding zero-day attacks is a hard problem with great potential for technology transfer. Self-aware detection systems [136, 137] include their own state in deciding whether a suspect is normal or an intruder. One way they may distinguish themselves from classical approaches is by identifying situations where an at-

tacker is provoking them into a DoS scenario with an otherwise benign circumstance. Also, self-aware detection systems may identify situations where the cost of the damage the adversary threatens is greater than stopping the hosted business functions and disconnecting the system. While biology, immunology and self-aware-inspired approaches are extensions of existing detection techniques that do not require a separate IDS technique category, These approaches are valuable in opening lines of investigation in the research area.

References

[1] G. Keizer, http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_ (September 2010).

[2] http://en.wikipedia.org/wiki/Stuxnet (2013).

[3] C. Bates, Hackers can gain access to medical implants and endanger patients' lives, http://www.dailymail.co.uk/health/article-2127568/Hackers-gain-access-medical-implants-endanger-patients-lives.html (April 2012).

[4] C. Hsu, Many Popular Medical Devices May Be Vulnerable to Cyber Attacks, http://www.medicaldaily.com/news/20120410/9486/medical-implants-pacemaker-hackers-cyber-attack-fda.htm (April 2012).

[5] http://www.esecurityplanet.com/network-security/european-power-grid-hit-by-cyber-attack.html.

[6] http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/.

[7] http://www.theregister.co.uk/2012/09/28/telvent_hack/.

[8] http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked/.

[9] http://security.blogs.cnn.com/2011/10/13/in-rare-admission-air-force-explains-and-downplays-drone-computer-virus.

[10] http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/.

[11] Z. Tao, A. Ruighaver, Wireless intrusion detection: Not as easy as traditional network intrusion detection, Region 10 Conference, Melbourne, Australia, 2005, pp. 1–5.

[12] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, H. Rhy, An experimental study of hierarchical intrusion detection for wireless industrial sensor networks, IEEE Transactions on Industrial Informatics 6 (4) (2010) 744–757.

[13] S.-Y. Chang, Y.-C. Hu, N. Laurenti, Simplemac: a jamming-resilient mac-layer protocol for wireless channel coordination, The 18th annual international conference on Mobile computing and networking, Istanbul, Turkey, 2012, pp. 77–88.

[14] J. Chiang, Y.-C. Hu, Dynamic jamming mitigation for wireless broadcast networks, The 27th Conference on Computer Communications, Phoenix, AZ, USA, 2008, pp. 1211–1219.

[15] A. Kashyap, T. Basar, R. Srikant, Correlated jamming on mimo gaussian fading channels, International Conference on Communications, Vol. 1, Paris, France, 2004, pp. 458–462.

[16] M. Strasser, S. Capkun, C. Popper, M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping, Symposium on Security and Privacy, Oakland, CA, USA, 2008, pp. 64–78.

[17] National Security Agency, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (2000).

[18] Z. Xiao, C. Liu, C. Chen, An anomaly detection scheme based on machine learning for wsn, 1st International Conference on Information Science and Engineering, Nanjing, China, 2009, pp. 3959–3962.

[19] D. Samfat, R. Molva, Idamn: an intrusion detection architecture for mobile networks, IEEE Journal on Selected Areas in Communications 15 (7) (1997) 1373–1380.

[20] J. Hall, M. Barbeau, E. Kranakis, Anomaly-based intrusion detection using mobility profiles of public transportation users, International Conference on Wireless And Mobile Computing, Networking And Communications, Vol. 2, Montreal, QC, Canada, 2005, pp. 17–24.

[21] D. Farid, M. Rahman, Learning intrusion detection based on adaptive bayesian algorithm, 11th International Conference on Computer and Information Technology, Khulna, Bangladesh, 2008, pp. 652–656.

[22] I. Svecs, T. Sarkar, S. Basu, J. Wong, Xidr: A dynamic framework utilizing cross-layer intrusion detection for effective response deployment, Computer Software and Applications Conference Workshops, 34th Annual, Seoul, South Korea, 2010, pp. 287–292.

[23] H. Han, X.-L. Lu, L.-Y. Ren, Using data mining to discover signatures in network-based intrusion detection, International Conference on Machine Learning and Cybernetics, Vol. 1, Beijing, China, 2002, pp. 13–17.

[24] A. Jones, S. Li, Temporal signatures for intrusion detection, Computer Security Applications Conference, New Orleans, LA, USA, 2001, pp. 252–261.

[25] Y. Ma, H. Cao, J. Ma, The intrusion detection method based on game theory in wireless sensor network, First International Conference on Ubi-Media Computing, Lanzhou University, China, 2008, pp. 326–331.

[26] S. Misra, P. Krishna, K. Abraham, Energy efficient learning solution for intrusion detection in wireless sensor networks, Second International Conference on Communication Systems and Networks, Bangalore, India, 2010, pp. 1–6.

[27] B. Foo, Y.-S. Wu, Y.-C. Mao, S. Bagchi, E. Spafford, Adepts: adaptive intrusion response using attack graphs in an e-commerce environment, International Conference on Dependable Systems and Networks, Yokohama, Japan, 2005, pp. 508–517.

[28] C. Ko, M. Ruschitzka, K. Levitt, Execution monitoring of security-critical programs in distributed systems: a specification-based approach, Symposium on Security and Privacy, Oakland, CA, USA, 1997, pp. 175–187.

[29] J. Shin, T. Kim, S. Tak, A reputation management scheme improving the trustworthiness of p2p networks, International Conference on Convergence and Hybrid Information Technology, Daejeon, South Korea, 2008, pp. 92–97.

[30] G. Bella, G. Costantino, S. Riccobene, Managing reputation over manets, Fourth International Conference on Information Assurance and Security, Naples, Italy, 2008, pp. 255–260.

[31] F. Li, N. Clarke, M. Papadaki, P. Dowland, Behaviour profiling on mobile devices, International Conference on Emerging Security Technologies, Canterbury, UK, 2010, pp. 77–82.

[32] http://en.wikipedia.org/wiki/Biometric (2012).

[33] F. Haddadi, M. Sarram, Wireless intrusion detection system using a lightweight agent, Second International Conference on Computer and Network Technology, Bangkok, Thailand, 2010, pp. 84–87.

[34] M. Drozda, I. Bate, J. Timmis, Bio-inspired Error Detection for Complex Systems, 17th Pacific Rim International Symposium on Dependable Computing, Pasadena, CA, USA, 2011, pp. 154–163.

[35] I. Onat, A. Miri, An intrusion detection system for wireless sensor networks, International Conference on Wireless And Mobile Computing, Networking And Communications, Vol. 3, Montreal, QC, Canada, 2005, pp. 253–259.

[36] http://www.thuraya.com.pk/space.html (2012).

[37] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, The 6th annual international conference on Mobile computing and networking, Boston, MA, USA, 2000, pp. 275–283.

[38] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection for discrete sequences: A survey, IEEE Transactions on Knowledge and Data Engineering 24 (5) (2012) 823–839.

[39] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: A survey, ACM Computing Surveys 41 (2009) 15:1–15:58.
[40] G. White, E. Fisch, U. Pooch, Cooperating security managers: a peer-based intrusion detection system, Network, IEEE 10 (1) (1996) 20–23.
[41] P. Porras, P. Neumann, EMERALD: Event monitoring enabling responses to anomalous live disturbances, The 20th National Information Systems Security Conference, Baltimore, MD, USA, 1997, pp. 353–365.
[42] P. Brutch, C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, Symposium on Applications and the Internet Workshops, Orlando, FL, USA, 2003, pp. 368–373.
[43] L. Ying, Z. Yan, O. Yang-jia, The design and implementation of host-based intrusion detection system, Third International Symposium on Intelligent Information Technology and Security Informatics, Jinggangshan, China, 2010, pp. 595–598.
[44] S. Zhong, T. Khoshgoftaar, S. Nath, A clustering approach to wireless network intrusion detection, 17th International Conference on Tools with Artificial Intelligence, Hong Kong, 2005, p. 196.
[45] `http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system` (2012).
[46] `http://en.wikipedia.org/wiki/Network_intrusion_detection_system` (2012).
[47] S. Buchegger, J. Y. Le Boudec, Performance analysis of the confidant protocol, The 3rd international symposium on Mobile ad hoc networking & computing, Lausanne, Switzerland, 2002, pp. 226–236.
[48] J. Liu, V. Issarny, Enhanced reputation mechanism for mobile ad hoc networks, Trust Management (2004) 48–62.
[49] F. Bao, I. R. Chen, M. Chang, J. Cho, Trust-based intrusion detection in wireless sensor networks, International Conference on Communications, Kyoto, Japan, 2011, pp. 1–6.
[50] I. R. Chen, F. Bao, M. Chang, J. Cho, Trust management for encounter-based routing in delay tolerant networks, Global Communications Conference, Miami, FL, USA, 2010, pp. 1–6.
[51] J. Cho, A. Swami, I. R. Chen, A survey on trust management for mobile ad hoc networks, IEEE Communications Surveys and Tutorials (2011) 1–22.
[52] F. Bao, I. R. Chen, M. Chang, J. H. Cho, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE Transactions on Network and Service Management 9 (2) (2012) 169–183.
[53] I. R. Chen, F. Bao, M. Chang, J. H. Cho, Integrated social and qos trust-based routing in delay tolerant networks, Wireless Personal Communications 66 (2012) 443–459.
[54] J. H. Cho, A. Swami, I. R. Chen, Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks, International Conference on Computational Science and Engineering, Vol. 2, Vancouver, Canada, 2009, pp. 641–650.
[55] J. H. Cho, A. Swami, I. R. Chen, Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks, Journal of Network and Computer Applications 35 (3) (2012) 1001–1012.
[56] F. Bao, I. R. Chen, M. Chang, J. H. Cho, Trust-Based Intrusion Detection in Wireless Sensor Networks, International Conference on Communications, Kyoto, Japan, 2011, pp. 1–6.
[57] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing, IEEE Transactions on Parallel and Distributed Systems (2014).
[58] W. Hairui, W. Hua, Research and design of multi-agent based intrusion detection system on wireless network, International Symposium on Computational Intelligence and Design, Vol. 1, Wuhan, China, 2008, pp. 444–447.
[59] R. Mitchell, I. R. Chen, M. Eltoweissy, Signalprint-based intrusion detection in wireless networks, Security in Emerging Wireless Communication and Networking Systems, Athens, Greece, 2010, pp. 77–88.
[60] Y. Mao, A semantic-based intrusion detection framework for wireless sensor network, 6th International Conference on Networked Computing, Gyeongju, South Korea, 2010, pp. 1–5.
[61] R. Mitchell, I. R. Chen, A hierarchical performance model for intrusion detection in cyber-physical systems, Wireless Communication and Networking Conference, Cancun, Mexico, 2011, pp. 2095–2100.
[62] R. Mitchell, I. R. Chen, On Survivability of Mobile Cyber Physical Systems with Intrusion Detection, Wireless Personal Communications 68 (2013) 1377–1391.
[63] R. Mitchell, I. R. Chen, Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems, IEEE Transactions on Reliability 62 (2013) 199–210.
[64] `http://www.ossec.net` (2012).
[65] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, The International Federation for Information Processing TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, Portoroz, Slovenia, 2002, pp. 107–121.
[66] Y. Yang, P. Zeng, X. Yang, Y. Huang, Efficient intrusion detection system model in wireless mesh network, Second International Conference on Networks Security Wireless Communications and Trusted Computing, Vol. 2, Wuhan, China, 2010, pp. 393–396.
[67] C. Mu, B. Shuai, H. Liu, Analysis of response factors in intrusion response decision-making, Third International Joint Conference on Computational Science and Optimization, Vol. 2, Anhui, China, 2010, pp. 395–399.
[68] D. Ragsdale, J. Carver, C.A., J. Humphries, U. Pooch, Adaptation techniques for intrusion detection and intrusion response systems, International Conference on Systems, Man, and Cybernetics, Vol. 4, Nashville, TN, USA, 2000, pp. 2344–2349.
[69] S. Yuan, Q. juan Chen, P. Li, Design of a four-layer ids model based on immune danger theory, 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, 2009, pp. 1–4.
[70] R. Sampangi, S. Dey, V. Viswanath, The sneeze algorithm: A social network amp; biomimetic approach for intrusion detection in wireless networks, International Workshop on Business Applications of Social Network Analysis, Bangalore, India, 2010, pp. 1–5.
[71] T. Stibor, R. Oates, G. Kendall, J. M. Garibaldi, Geometrical insights into the dendritic cell algorithm, The 11th Annual conference on Genetic and evolutionary computation, GECCO '09, Montreal, QC, Canada, 2009, pp. 1275–1282.
[72] J. Yang, Y. Ge, H. Xiong, Y. Chen, H. Liu, Performing Joint Learning for Passive Intrusion Detection in Pervasive Wireless Environments, International Conference on Computer Communications, San Diego, CA, USA, 2010, pp. 1–9.
[73] B. Moyers, J. Dunning, R. Marchany, J. Tront, The Multi-Vector Portable Intrusion Detection System (MVP-IDS): A hybrid approach to intrusion detection for portable information devices, International Conference on Wireless Information Technology and Systems, Honolulu, HI, USA, 2010, pp. 1–4.
[74] T. OConnor, D. Reeves, Bluetooth Network-Based Misuse Detection, Annual Computer Security Applications Conference, Anaheim, CA, USA, 2008, pp. 377–391.
[75] A. da Silva, Decentralized intrusion detection in wireless sensor networks, 1st international workshop on quality of service & security in wireless and mobile networks, Montreal, QC, Canada, 2005, pp. 16–23.
[76] S. Rajasegarar, J. C. Bezdek, C. Leckie, M. Palaniswami, Elliptical anomalies in wireless sensor networks, ACM Transactions on Sensor Networks 6 (1) (2010) 7:1–7:28.
[77] A. Boukerche, X. Li, An agent-based trust and reputation management scheme for wireless sensor networks, Global Telecommunications Conference, St. Louis, MO, USA, 2005, pp. 1–5.
[78] A. Boukerch, L. Xu, K. El-Khatib, Trust-based security for wireless ad hoc and sensor networks, Computer Communica-

tions 30 (11-12) (2007) 2413–2427.
[79] J. Hur, Y. Lee, S.-M. Hong, H. Yoon, Trust management for resilient wireless sensor networks, in: D. Won, S. Kim (Eds.), Information Security and Cryptology, Vol. 3935 of Lecture Notes in Computer Science, 2006, pp. 56–68.
[80] S. Ganeriwal, L. K. Balzano, M. B. Srivastava, Reputation-based framework for high integrity sensor networks, ACM Transactions on Sensor Networks 4 (2008) 15:1–15:37.
[81] H. Chen, Task-based trust management for wireless sensor networks, International Journal of Security and Its Applications 3 (2) (2009) 21–26.
[82] M. Zamani, M. Movahedi, M. Ebadzadeh, H. Pedram, A DDOS-aware ids model based on danger theory and mobile agents, International Conference on Computational Intelligence and Security, Vol. 1, Beijing, China, 2009, pp. 516–520.
[83] K. Ioannis, T. Dimitriou, F. Freiling, Towards intrusion detection in wireless sensor networks, The 13th European Wireless Conference, Paris, France, 2007.
[84] S. Sarafijanović, J. Y. Boudec, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors, in: G. Nicosia, V. Cutello, P. Bentley, J. Timmis (Eds.), Artificial Immune Systems, Vol. 3239 of Lecture Notes in Computer Science, 2004, pp. 342–356.
[85] Y. Zhang, W. Lee, Y.-A. Huang, Intrusion detection techniques for mobile wireless networks, Wireless Networks 9 (5) (2003) 545–556.
[86] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer, R. Kemmerer, An intrusion detection tool for aodv-based ad hoc wireless networks, 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, 2004, pp. 16–27.
[87] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, K. Levitt, A specification-based intrusion detection system for aodv, 1st workshop on Security of ad hoc and sensor networks, Fairfax, VA, USA, 2003, pp. 125–134.
[88] G. Jacoby, R. Marchany, I. Davis, N.J., Battery-based intrusion detection a first line of defense, The Fifth Annual Systems, Man, and Cybernetics Information Assurance Workshop, The Hague, The Netherlands, 2004, pp. 272–279.
[89] T. Martin, M. Hsiao, D. Ha, J. Krishnaswami, Denial-of-service attacks on battery-powered mobile computers, The Second Annual Conference on Pervasive Computing and Communications, Orlando, FL, USA, 2004, pp. 309–318.
[90] D. Castle, A. Darensburg, B. Griffin, T. Hickman, S. Warders, G. Jacoby, Gibraltar: A mobile host-based intrusion protection system, National Conference on Undergraduate Research, Asheville, NC, USA, 2006.
[91] P. Kannadiga, M. Zulkernine, S. Ahamed, Towards an intrusion detection system for pervasive computing environments, International Conference on Information Technology: Coding and Computing, Vol. 2, Las Vegas, NV, USA, 2005, pp. 277–282.
[92] X. Wang, J. Wong, F. Stanley, S. Basu, Cross-layer based anomaly detection in wireless mesh networks, Ninth Annual International Symposium on Applications and the Internet, Seattle, WA, USA, 2009, pp. 9–15.
[93] H. Li, M. Xu, Y. Li, The research of frame and key technologies for intrusion detection system in ieee 802.11-based wireless mesh networks, International Conference on Complex, Intelligent and Software Intensive Systems, Barcelona, Spain, 2008, pp. 455–460.
[94] J. Zhou, Z. Chen, W. Jiang, Probability based ids towards secure wmn, 2nd International Workshop on Intelligent Systems and Applications, Wuhan, China, 2010, pp. 1–4.
[95] C.-H. Tsang, S. Kwong, Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction, International Conference on Industrial Technology, Hong Kong, 2005, pp. 51–56.
[96] `http://www.snort.org` (2012).
[97] P. Uppuluri, R. Sekar, Experiences with specification-based intrusion detection, in: W. Lee, L. M, A. Wespi (Eds.), Recent Advances in Intrusion Detection, Vol. 2212 of Lecture Notes in Computer Science, 2001, pp. 172–189.
[98] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou, Specification-based anomaly detection: a new approach for detecting network intrusions, 9th conference on Computer and communications security, CCS '02, Washington, DC, USA, 2002, pp. 265–274.
[99] S. Hofmeyr, S. Forrest, A. Somayaji, Intrusion detection using sequences of system calls, Journal of Computer Security 6 (3) (1998) 151–180.
[100] W. Lee, S. Stolfo, Data mining approaches for intrusion detection, The 7th conference on USENIX Security Symposium-Volume 7, USENIX Association, New Orleans, LA, USA, 1998, p. 6.
[101] R. Mitchell, I. R. Chen, Behavior rule based intrusion detection for supporting secure medical cyber physical systems, International Conference on Computer Communication Networks, Munich, Germany, 2012.
[102] R. Berthier, W. Sanders, Specification-based intrusion detection for advanced metering infrastructures, 17th Pacific Rim International Symposium on Dependable Computing, Pasadena, CA, USA, 2011, pp. 184–193.
[103] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, S. Sastry, Attacks against process control systems: risk assessment, detection, and response, The 6th Symposium on Information, Computer and Communications Security, Hong Kong, China, 2011, pp. 355–366.
[104] Y. Chen, B. Luo, S2a: secure smart household appliances, The second conference on Data and Application Security and Privacy, San Antonio, TX, USA, 2012, pp. 217–228.
[105] P. Jokar, H. Nicanfar, V. Leung, Specification-based intrusion detection for home area networks in smart grids, International Conference on Smart Grid Communications, Brussels, Belgium, 2011, pp. 208–213.
[106] R. Klump, M. Kwiatkowski, Distributed ip watchlist generation for intrusion detection in the electrical smart grid, Critical Infrastructure Protection IV 342 (2010) 113–126.
[107] B. Luitel, G. Venayagamoorthy, C. Johnson, Enhanced wide area monitoring system, Innovative Smart Grid Technologies, Gaithersburg, MD, USA, 2010, pp. 1–7.
[108] C.-W. Ten, J. Hong, C.-C. Liu, Anomaly detection for cybersecurity of the substations, IEEE Transactions on Smart Grid 2 (4) (2011) 865–873.
[109] X. Wang, P. Yi, Security framework for wireless communications in smart distribution grid, IEEE Transactions on Smart Grid 2 (4) (2011) 809–818.
[110] Y. Wang, D. Ruan, J. Xu, M. Wen, L. Deng, Computational intelligence algorithms analysis for smart grid cyber security, in: Y. Tan, Y. Shi, K. Tan (Eds.), Advances in Swarm Intelligence, Vol. 6146 of Lecture Notes in Computer Science, 2010, pp. 77–84.
[111] R. A. Clarke, R. Knake, Cyber War: The Next Threat to National Security and What to Do About It, Ecco Press, 2010.
[112] D. Sanger, E. Bumiller, Pentagon to consider cyberattacks acts of war, The New York Times.
[113] R. Mitchell, I. R. Chen, Adaptive Intrusion Detection for Unmanned Aircraft Systems based on Behavior Rule Specification, IEEE Transactions on Systems, Man and Cybernetics (2013) 1–10.
[114] R. Mitchell, I. R. Chen, Behavior Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications, IEEE Transactions on Smart Grid (2013) 1–12.
[115] R. Mitchell, I. R. Chen, Specification based intrusion detection for unmanned aircraft systems, MobiHoc Workshop on Airborne Networks and Communications, Hilton Head Island, SC, USA, 2012, pp. 31–36.
[116] F. B. Bastani, I. R. Chen, T. W. Tsao, Reliability of systems with fuzzy-failure criterion, Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 442–448.
[117] I. R. Chen, F. B. Bastani, Effect of artificial-intelligence

planning-procedures on system reliability, IEEE Transactions on Reliability 40 (3) (1991) 364–369.
[118] I. R. Chen, F. B. Bastani, T. W. Tsao, On the reliability of AI planning software in real-time applications, IEEE Transactions on Knowledge and Data Engineering 7 (1) (1995) 4–13.
[119] I. R. Chen, D. C. Wang, Analyzing Dynamic Voting using Petri Nets, 15th IEEE Symposium on Reliable Distributed Systems, Niagara Falls, Canada, 1996, pp. 44–53.
[120] J. H. Cho, I. R. Chen, P. G. Feng, Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks, IEEE Transactions on Reliability 59 (1) (2010) 231–241.
[121] I. R. Chen, D. C. Wang, Analysis of replicated data with repair dependency, The Computer Journal 39 (9) (1996) 767–779.
[122] E. Y. Vasserman, N. J. Hopper, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks, IEEE Transactions on Mobile Computing, 12 (2) (2013) 318–332.
[123] R. V. Boppana, X. Su, On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, 10 (8) (2011) 1162–1174.
[124] I. R. Chen, T.-M. Chen, C. Lee, Performance evaluation of forwarding strategies for location management in mobile networks, The Computer Journal 41 (4) (1998) 243–253.
[125] B. Gu, I. R. Chen, Performance Analysis of Location-Aware Mobile Service Proxies for Reducing Network Cost in Personal Communication Systems, Mobile Networks and Applications 10 (4) (2005) 453–463.
[126] I. Khalil, S. Bagchi, Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure, IEEE Transactions on Mobile Computing, 10 (8) (2011) 1096–1113.
[127] Y. Li, I. R. Chen, Design and Performance Analysis of Mobility Management Schemes Based on Pointer Forwarding for Wireless Mesh Networks, Transactions on Mobile Computing 10 (3) (2011) 349–361.
[128] I. R. Chen, A. Speer, M. Eltoweissy, Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks, Transactions on Dependable and Secure Computing 8 (2) (2011) 161–176.
[129] H. Al-Hamadi, I. R. Chen, Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks, Transactions on Network and Service Management 10 (2) (2013) 189–203.
[130] E. Ayday, F. Fekri, An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks, IEEE Transactions on Mobile Computing 11 (9) (2012) 1514–1531.
[131] H. Zhu, S. Du, Z. Gao, M. Dong, Z. Cao, A Probabilistic Misbehavior Detection Scheme Towards Efficient Trust Establishment in Delay-Tolerant Networks, IEEE Transactions on Parallel and Distributed Systems 25 (2) (2014) 22–32.
[132] O. Yilmaz, I. R. Chen, Utilizing call admission control for pricing optimization of multiple service classes in wireless cellular networks, Computer Communications 32 (2) (2009) 317–323.
[133] I. R. Chen, T. H. Hsi, Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers, Performance Evaluation 33 (2) (1998) 89–112.
[134] S.-T. Cheng, C.-M. Chen, I. R. Chen, Dynamic quota-based admission control with sub-rating in multimedia servers, Multimedia Systems 8 (2) (2000) 83–91.
[135] R. Mitchell, Design and Analysis of Intrusion Detection Protocols in Cyber Physical Systems, Ph.D. thesis, Virginia Tech (2013).
[136] A. Bronstein, J. Das, M. Duro, R. Friedrich, G. Kleyner, M. Mueller, S. Singhal, I. Cohen, Self-aware services: using Bayesian networks for detecting anomalies in Internet-based services, International Federation for Information Processing International Symposium on Integrated Network Management, Seattle, WA, USA, 2001, pp. 623–638.
[137] S. Ganeriwal, A. Kansal, M. Srivastava, Self aware actuation for fault repair in sensor networks, International Conference on Robotics and Automation, Vol. 5, New Orleans, LA, USA, 2004, pp. 5244–5249.