Security in Distributed, Grid, and Pervasive Computing
Yang Xiao,(Eds.) pp. – - –

Chapter 6

Intrusion Detection in Wireless Sensor Networks

Fereshteh Amini
Department of Computer Science
University of Manitoba, Winnipeg, Manitoba, Canada
E-mail: amini@cs.umanitoba.ca

Vojislav B. Mišić
Department of Computer Science
University of Manitoba, Winnipeg, Manitoba, Canada
E-mail: vmisic@cs.umanitoba.ca

Jelena Mišić
Department of Computer Science
University of Manitoba, Winnipeg, Manitoba, Canada
E-mail: vmisic@cs.umanitoba.ca

1 Abstract

Security is rapidly replacing performance as the first and foremost concern in many networking scenarios. This includes wireless sensor networks which are becoming increasingly popular for many environmental, logistics, engineering, health, and military applications. While security prevention is important, it cannot guarantee that attacks will not be launched and that, once launched, they will not be successful. Therefore, detection of malicious intrusions forms an important part of an integrated approach to security. In this Chapter, we review the basic tenets of intrusion detection in wireless sensor networks. We present the main differences between wireless sensor networks and other similar networks such as ad hoc networks, and discuss

the manner in which these differences limit and guide the analysis and development of viable and effective approaches to intrusion detection. We also present a survey of current research in this area, and outline main challenges for future research.

2 Introduction

Wireless sensor networks (WSNs) consist of a large number of tiny sensor devices or nodes with sensing, computational, and communication capabilities. Sensor nodes monitor some physical phenomena in their environment, record the values of appropriate variables, and send them using wireless transmission toward one (or, in some cases, several) network sinks. Along the way, data may pass through a number of intermediate nodes where some filtering and aggregation may be performed. Network sinks act as gateways which collect the data, possibly aggregate it, and pass it on to the sensing applications that requested it. Sensor nodes are small and possess limited energy, memory, bandwidth, and processing power. They can be deployed in inhospitable places, with little or no human intervention thereafter. A sensor network is (or should be) able to operate autonomously, from the moment sensor nodes as deployed in the space of interest to the time when batteries are exhausted and sensor nodes stop working. they are deployed to the exhaustion This generic scenario may be applied in many situations, and it should come as no surprise that wireless sensor networks are becoming increasingly popular in many environmental, business, engineering, healthcare, military, surveillance, and other applications [2].

However, the intrinsic characteristics of WSNs make them vulnerable to attacks by malicious intruders. In military and surveillance applications, sensor networks can provide crucial data to their operators, and degrading their performance or even subverting them may offer generous benefits to an adversary. Therefore, security issues are of primary concern for the design and deployment of wireless sensor networks.

Typically, security implies intrusion prevention through physical protection of the system, advanced cryptographic techniques, and appropriate security policies. However, wireless sensor networks are often expected to operate unattended for prolonged periods of time. On account of that, the importance of security policies is much less pronounced than for systems that include a significant human component, such as information systems and online applications. For that same reason, and because the sensor net-

work often operates in places where an adversary can easily access the actual devices, physical protection of sensor devices is often impossible. As a result, we have to rely on cryptographic techniques for attack prevention, and this is not enough. Or, in other words, despite our best efforts in devising secure protocols and communication techniques to protect against attacks, we cannot really expect that the network will be able to resist all possible attacks.

Consequently, we have to consider not just intrusion prevention techniques as the first line of defence, but also the techniques to detect ongoing attacks and techniques to eliminate or, at least, diminish the impact of such attacks. The former techniques, which are collectively known as *intrusion detection*, form the second line of defence and they are the focus of this Chapter; the latter belong to a wider range of security response policies which are not discussed here, although occasional recommendations will be made in relationship with particular intrusion detection techniques.

The Chapter is organized as follows. First, we review the main characteristics of wireless sensor networks in more detail, and outline the reasons for which intrusion detection techniques developed for other types of wireless networks are not readily applicable to wireless sensor networks. Then, we present the possible criteria for classification of intrusion detection techniques and discuss their advantages and shortcomings. A brief overview of some of the techniques proposed in the literature follows. Finally, we outline the challenges for research in this area and discuss some promising avenues for future work.

3 Why Wireless Sensor Networks Are Difficult to Protect

As mentioned above, wireless sensor nodes are typically small, battery operated devices with three main subsystems:

- The sensing subsystem consists of one or more sensors or transducers which convert the monitored physical variable to an electrical, possibly digital, signal.

- The computational subsystem is a small microcontroller with integrated memory; it control the operation of the other two subsystems.

- The communication or radio subsystem enables the node to communicate with other nodes in its vicinity through wireless transmissions.

Three main problems that make wireless sensor networks difficult to protect and secure against intrusions can be readily identified. First problem is the very nature of the wireless communication medium, which makes wireless communication inherently insecure. Unlike wired networks, where a device has to be physically connected to the medium, the wireless medium is open and accessible to anyone. Moreover, the range in which the impact of an intruder can be felt primarily depends on the characteristics of intruder's equipment; an intruder with a strong transmitter can easily produce interference from a distance which makes any physical response infeasible or, in some applications, plain impossible.

The second problem is the absence of any fixed infrastructure – in particular, there is no central or master controller to monitor the operation of the network and analyze the data to detect intrusions. While most such networks have a designated network sink, its role is typically restricted to data collection and query distribution, and does not include any form of actual control. As a result, any intrusion detection technique has to be implemented as a cooperative, distributed effort of many among the nodes in the sensor network, or even all of them together. An added difficulty stems from the unstable topology of the network, which may be due to battery exhaustion or (in some cases) node mobility.

Yet other wireless networks exist that have both of these problems: wireless ad hoc networks. In those networks, wireless communication medium is used, and they operate with little infrastructure or none at all. A number of intrusion prevention techniques has been proposed for such networks [10], and also a few techniques for intrusion detection [5, 17, 28, 29]. Such techniques are a combination of several approaches, including use of cooperating mobile agents [6, 15], possibly combined with the analysis of audit logs [13], a game-theoretic approach [1], and a number of others.

However, the main problem with wireless sensor networs lies elsewhere: in their limited computational and communication resources. Namely, wireless sensor networks need to operate autonomously for prolonged periods of time, and they have to run on battery power. To cater to those goals, the energy consumption of sensor nodes has to be minimized; this necessitates both the power efficiency of the hardware (and its small size) and the efficiency of communications protocols and the software that implements those protocols. The processing subsystem is invariably implemented with a small

microprocessor with limited resources, which runs at low clock speeds, and thus offers only modest computational and memory capabilities. As a result,

- The processing power of such subsystems is generally insufficient to run a full-scale software agent dedicated to intrusion detection [29].
- Even if sufficient computational capability were available, the low data rate of typical communication channels—250kbps for IEEE 802.15.4 networks operating in the ISM band at 2.4GHz, but only 20 or 40 kbps when operating in other bands [12]—simply does not suffice for the rather intense communication that those agents need.
- By the same token, any substantial computation is infeasible.
- Moreover, since memory capacity is of the order of hundreds or, at best, thousands of bytes, an audit log of realistic size cannot be maintained.
- Simple and efficient protocols mean that individual layers which are traditionally observed in wired networks (but also in other wireless networks) [24] must be integrated; after all, a wireless sensor network is a highly specialized network for limited class of applications, and such integration makes perfect sense in view of the inherent limitations of wireless sensor networks [2]. The important implication is that existing techniques which focus on one layer only—for example, routing [3, 18] or media access control (MAC) [26]—cannot readily be applied.

Further problems pertinent to wireless sensor network include

- Sensor networks have a large number of nodes, which may exceed hundreds or even thousands [2]. Security architectures developed for small scale ad hoc networks are infeasible for resource-limited large-scale sensor networks.
- Sensor networks exhibit comparatively stable communication patterns as opposed to ad hoc networks. In ad hoc networks, nodes are assumed to communicate among themselves and traffic patterns are reasonably random. On the contrary, in sensor networks most of the traffic is created as many-to-one nearly-periodic transmission, as nodes have to report sensor readings to a central, more capable node.

- In ad hoc networks, communications are generally of the point-to-point, and often of multi-hop, variety. There is no fixed source or destination of packets; instead, roles change over time. The only exception might be slightly increased traffic to and from nodes which act as access points to the wired network. In sensor networks, data flow is directional and there is a single common destination for most, if not all, traffic flows.

- Sensor devices are physically vulnerable – they are susceptible to being damaged, captured and subverted (perhaps through reprogramming), or simply destroyed by the attacker.

The inescapable conclusion is that existing solutions for intrusion detection cannot be re-used directly; instead, they have to be adapted to the characteristics of wireless sensor networks [6, 14, 22]. In particular, intrusion detection, like other security-related challenges, requires an integrated and comprehensive approach; if added as an afterthought, it cannot be as effective [21].

That makes us particularly hard to design an ideal security architecture for the whole layers. In practical applications, we should design our protocols in each layer with security in mind. Before security considerations, there exist several protocols in every layer. But when it comes to the security, we should incorporate the security method into already existing protocol or cooperate with them. The consequence is that the original architecture works inefficiently or otherwise should be redesigned.

4 Security Considerations

As is well known [4], main aspects of security include the following:

- Authentication is necessary to enable sensor nodes to detect maliciously injected or spoofed packets. It enables a node to verify the origin of a packet and ensure data integrity. Almost all applications require data authentication. In many applications, military as well as civilian ones, an adversary has clear incentives to join the network in order to inject false information such as fake data or routing information. Although authentication tries to prevent outsiders from injecting or spoofing packets, it does not solve the problem of compromised nodes. Since an attacker may have access to the secret keys of

a compromized node, it can authenticate itself to the network. However, we may be able to use intrusion detection techniques to find the compromised nodes and revoke their cryptographic keys network-wide.

- Confidentiality or secrecy of data communications prevents unauthorized users from learning the contents of the messages. To that end, we can use standard encryption functions which might include secret keys shared among the communicating parties. (Note that the use of public-private key cryptography, while much more resilient to attacks, is out of the question on account of limited computational resources of sensor nodes.) However, encryption itself is not sufficient for protecting the privacy of data, as an eavesdropper can perform traffic analysis on the overheard cipher text, and this can release sensitive information about the data. In addition to encryption, privacy of sensed data also needs to be enforced through access control policies at the base station to prevent misuse of information.

- Availability requires that the sensor network is functional throughout its lifetime. Denial of Service (DoS) attacks result in a loss of availability [26]. In practice, loss of availability may have serious impacts. In a manufacturing monitoring application, loss of availability may cause failure to detect a potential accident and result in financial loss; in a battlefield surveillance application, loss of availability may open a back door for enemy invasion. Various attacks can compromise the availability of the sensor network. When considering availability in sensor networks, it is important to achieve graceful degradation in the presence of node compromise or benign node failures.

- Integrity of services is another security requirement. Above the networking layer, the sensor network usually implements several application-level services. Data aggregation is one of the most important sensor network services. In data aggregation, a sensor node collects readings from neighboring nodes, aggregates them, and sends them to the base station or another data processing node. The goal of secure data aggregation is to obtain a relatively accurate estimate of the real-world quantity being measured, and to be able to detect and reject a reported value that is significantly distorted by corrupted nodes.

5 Classifying the Intrusions

Intrusion attacks can be categorized according to different criteria.

5.1 Location of the attacker with respect to the network

According to this criterion, attacks can be classified into insider and outsider attacks. In an outsider attack, the attack node is not an authorized participant of the sensor network. As the sensor network communicates over a wireless channel, a passive attacker can easily eavesdrop on the used frequency range to steal private or sensitive information. The adversary can also alter or spoof packets to attack the authenticity of communication or inject interfering wireless signals to jam the network. Another form of outsider attack is to disable sensor nodes. An attacker can inject useless packets to drain the receivers battery, or he can capture and physically destroy nodes. A failed node is similar to a disabled node.

Unlike outsider attacks, insider attacks are performed by compromised nodes in the WSN. With node compromise, an adversary can perform an insider attack. In contrast to disabled node, compromised node generally seeks to disrupt or paralyze the network. A compromised node may be a subverted sensor node or a more powerful device, like laptop, with more computational power, memory, and powerful radio. It may be running some malicious code and seek to steal secrets from the sensor network or disrupt its normal functions. It may have a radio compatible with sensor nodes such that it can communicate with the sensor network.

5.2 Networking layer in which the attack takes place

Attacks on wireless sensor networks can occur in different networking layers such as application, data link, network and physical layers, or in two or more of these layers simultaneously.

Attacks on the physical layer are, in fact, the easiest to launch. Since wireless sensor networks can be deployed in hostile environment or densely populated areas, physical access to individual nodes is possible. Even casual passers-by may be able to damage, destroy, or tamper with sensor devices. Destruction of the node could cause gaps in sensor or communication coverage. Better equipped attackers can interrogate a devices memory, stealing its data or cryptographic keys. The code can be replaced with a malicious

program which is potentially undetectable to neighboring nodes. The capability profile of the subverted node becomes a fully authorized insider.

Attacks on the data link layer , including the media access control layer, are also comparatively simple. Many data link protocols in wireless sensor networks just consider the efficiency and fairness of utilizing the common channel. In these protocols, all the nodes in the network follow the same set of rules to access the media. For these reasons, many data link protocols are very vulnerable. Currently known attacks on the data link layer are mainly focused on the channel access. That's to say, the malicious node could randomly access to the link and transmit or eavesdrop messages from the channel. More seriously, this node may inject and alter transmitted data. These attacks can be organized in three categories: collision attack, unfairness attack, and exhaustion attack.

- Collision Attack: Each node could inform its neighbors that he has some data to send or receive by exchanging RTS (Request To Send)/CTS (Clear To Send) control packets. Neighbor nodes could detect that the public channel is busy, and they would back off their sending even if they have some data packets to send. Using this mechanism, the collision only happens in the exchanging period of RTS and CTS packets, which means the data packet sending process is a non-collision process. In addition, each node will check whether the channel is busy or idle before sending RTS and CTS packets. Thats why the probability of collision is very low. Under the condition, when there is a packet transmitting on channel, adversaries can easily conduct attacks through sending out some packets to disrupt it(such as data packs, control packets sent by normal nodes).

- Unfairness Attack: For most RTS/CTS-based data link protocols, each node has the same priority to get the common channel. The rule is that the first tried node gets hold of the channel. Besides, all other nodes have to wait for a random length time before trying to transmit packets. This rule could ensure that every node accesses common channel fairly. Adversaries could utilize these characteristics to attack the network. They send out packets just waiting for a very short time or without waiting. This causes the common channel used more by adversaries than by normal nodes.

- Exhaustion Attack: RTS/CTS based data link protocols are sender invitation data link protocols. That is, when a sender sends out RTS control packet to start a transmission, the receiver has to acknowledge the invitation with CTS control packet if it is available. Since adversaries are also normal nodes, the receiver can not exactly distinguish whether the RTS packet was sent by normal nodes or by adversaries. Under this condition, adversaries can attempt to retransmit RTS control packets to normal nodes repeatedly, enforcing receiver to acknowledge them incessantly. These kinds of abnormal retransmissions could result in the exhaustion of battery resources of receivers.

Attacks on Network Layer It is not enough to secure our sensor networks by only using the data link layer security countermeasures. Those countermeasures can only protect against the outsider attacks. Some insider attacks which can not be defended against in the link layer involve the routing protocols in the sensor networks [14]. These attacks can be categorized into the following kinds: selective forwarding, sinkhole attacks, wormhole attacks, Sybil attacks, and HELLO flood attacks:

- In sensor networks, each node can act as a router, that is to say, it could forward messages received. In **selective forwarding** attacks, once a middle node is captured by a malicious node, this node may refuse to forward certain messages and simply drop them. This behaves like a black hole. In practical applications, the malicious nodes use the attack to modify the packets. The neighboring nodes will conclude that the compromised node has failed and decide to seek another route skipping this node.

- In **sinkhole** attacks, the malicious node's goal is to lure all the traffics from a particular area to gain the entire message from the inspect area. The motivation of a sinkhole attack is that it makes selective forwarding trivial. By transmitting all traffic to the base station, the adversary can easily modify packets origination from any node in the area.

- In **wormhole** attacks, the powerful adversary is usually close to a base station. Remote powerful nodes are often colluded to establish an artificial links to transmit packets the remote nodes collected. Since these packets are originated the base station, all the packets may be

captured by the adversary. So the wormhole usually happens with the sinkhole. The sinkhole and wormhole attacks can be difficult to detect.

- In **Sybil** attack, the adversary presents multiple identities to other nodes in the network. So if other nodes are fooled, the data flow will be transmitted through the adversary and the control of substantial fractions of the network system will be in risk [7].

- In **HELLO** attacks, since all nodes have to send HELLO packets to neighbor nodes before the network established. A powerful adversary could use this characteristic to send HELLO packets to all nodes thus destroy the network.

Some or all of these attacks can be combined to attack the current routing protocols, for example, TinyOS beaconing protocol is used to construct the topology through a broadcast message from the base station and the rebroadcast message from the node who received the message. An adversary with the ability of powerful transmission may replace the base station. If authentication is introduced, another adversary which situated near the base station can launch a wormhole and sinkhole attack. Also, the adversary can use HELLO flood to make itself as a parent of other node in the network.

Attacks on Application Layer The most common kind of application level attack is the Denial of Services (DoS) attack [26, 16]. A DoS attack is any event that diminishes or eliminates a networks capability to perform its expected functions. It is the general result of any action that prevents any part of a WSN from functioning correctly or in a timely manner. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS.

6 Intrusion Detection

As noted above, intrusion prevention techniques (which typically use encryption and authentication) are generally insufficient to ensure security, and must be complemented with intrusion detection [10]. However, close collaboration of those techniques would allow the latter to make use of the information provided by the former and vice versa, and thus improve the efficiency of both of them [11].

Detection technique An Intrusion Detection System (IDS) may be classified on the basis of its detection technique [4]. The main techniques include:

- A potential intrusion is reported by **Misuse or Signature-based** detection if a sequence of events within a system matches a set of known security policy violations. In order to detect an intrusion by Misuse model a knowledge of potential vulnerabilities of the system should be available. The intrusion detection system then applies this rule set to the sequences of data to determine a possible intrusion. This technique may exhibit low false positives, but does not perform well at detecting previously unknown attacks. Subhadrabandhu et al. [25] present a robust intrusion detection using misuse detection techniques. Anjum et al. [3] deal with the ability of various routing protocols to facilitate intrusion detection techniques when the attack signatures are completely known in network.

- **Anomaly** detection uses a set of expected values to compare with system's behavior. If the computed statistics do not match the expected values, an anomaly is reported. Anomaly-based detection defines a profile of normal behavior and classifies any deviation of that profile as an intrusion. The normal profile is updated as the system learns the subjects behavior. This technique may detect previously unknown attacks but may exhibit high false positives. Zhang et al. [28], present an anomaly detection model. They use trace data which describes the normal updates of routing information Since, the main concern is that false routing will be used by other nodes. The generated trace data will then bear evidence of normality or anomaly. High false positive rates are reported based on their simulation results.

  Anomaly detection may be used to detect attacks against a network daemon or a SetUID program by building a normal profile of the system calls made during program execution. If the process execution deviates significantly from the established profile, an intrusion is assumed. Okazaki et al. [19] have proposed a lightweight approach using profiles consisting of the type of system call and its frequency occurrence, in which speech recognition methods is used to calculate the optimal match between a normal profile and a sample profile.

- Compared to the Misuse modeling, **specification** modeling takes the opposite approach; it looks for specification of how a system or program executes and marks a sequence of instructions as a potential

intrusion if it violates the specification. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate. For example, Snort [23] is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature-based and anomaly-based detection methods.

Location of the Intrusion Detection System A second distinction can be made in terms of the placement of the IDS. In this respect IDSs are usually divided into host-based and network-based systems and once again, both systems offer the advantages and disadvantages:

- Host-based systems are present on each host that requires monitoring, and collect data concerning the operation of this host, usually log files, network traffic to and from the host, or information on processes running on the host. Host-based systems are able to determine if an attempted attack was indeed successful, and can detect local attacks, privilege escalation attacks and attacks which are encrypted. However, such systems can be difficult to deploy and manage, especially when the number of hosts needing protection is large. Furthermore, these systems are unable to detect attacks against multiple targets within the network.

- Network-based IDSs monitor the network traffic on the network containing the hosts to be protected, and are usually run on a separate machine termed a sensor. Network-based systems are able to monitor a large number of hosts with relatively little deployment costs, and are able to identify attacks to and from multiple hosts. However, they are unable to detect whether an attempted attack was indeed successful, and are unable to deal with local or encrypted attacks.

Hybrid systems, which incorporate host- and network-based elements can offer the best protective capabilities, and systems to protect against attacks from multiple sources are also under development.

7 Approaches to Intrusion Detection

Although wireless sensor networks belong to the general family of wireless or Mobile Ad-hoc NETworks (MANETs), they have their own distinctive

features. Many works [5, 11, 28] have investigated various aspects related to security and intrusion detection in MANETs but few in WSNs. The main differences between the MANETs and sensor networks from the security viewpoint can be summarized as follows:

- **Simpler device characteristics:** Sensor nodes are small and inexpensive devices with restricted transmit power (short range) and energy supplies. Due to low computation and communication capabilities authentication and encryption based security solutions are difficult to implement in a large scale sensor network. Unlike typical mobile devices, sensor nodes spend a considerable amount of energy not only while sending and receiving data but also in the listening mode. Thus, sensor networks are more vulnerable to resource depletion attacks.

- **Lack of mobility:** In most applications, sensor nodes are stationary. They stay put wherever they are deployed. This decreases routing overhead. Most important, in sensor networks, route request broadcasts of reactive routing protocols and periodic updates of proactive routing protocols either do not occur or occur much less frequently.

- **Large network size:** Sensor networks consist of large numbers of nodes.

These differences make the IDS solutions proposed for MANETs, unsuitable for WSNs. The challenges for an IDS in WSN are mainly due to the lack of resources. Besides, methods developed to be used in traditional networks cannot be applied directly to WSNs, since they demand resources not available in sensor networks.

WSNs are typically application oriented, which means they are designed to have very specific characteristics according to the target application. The intrusion detection assumes that the normal system behavior is different from the behavior of a system under attack. The several possible WSN configurations make, the definition of the usual or expected system behavior, difficult.

Since common nodes are designed to be cheap and small, they have limited hardware resources. Thus, the available memory may not be sufficient to create a detection log file. Moreover, a sensor node is designed to be disposed after being used by the application and it makes difficult to recover a log file due to the possible dangerous environment in which the network

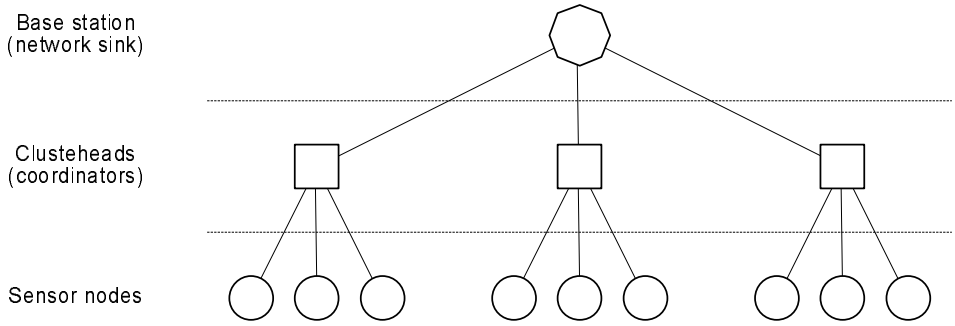

Figure 1: Hierarchical Architecture for Intrusion Detection in WSN.

was deployed. The software stored in the node must be designed to save as much energy as possible in order to extend the network lifetime.

Finally, another challenge to the design of an IDS is the frequent failures of sensor nodes when compared to processing entities found in wired networks. Given all these characteristics, it is important to detect the intrusions in real time. In this way, we could hold the intruder and minimize the possible damages.

7.1 Intrusion Detection Architecture for WSN

The optimal intrusion detection architecture for a WSN demands to be both distributed and at the same time, hierarchical for the special characteristics of this kind of network which we mentioned earlier. Distributed architecture allows detecting distributed attacks and provides scalability and robustness since it has different views of the network. Using this architecture, we can also distribute the process of detecting an intrusion over several nodes in the network. Because this architecture relies on cooperative work of nodes and is not centralized, it can be very fault tolerant and that is to say if a node is removed from the network for any reason, the intrusion detection can still work properly.

Figure 1 shows a hierarchical architecture for intrusion detection in WSN. The intrusion detection architecture mimics the hardware architecture of WSN in which intrusion detection is done in three levels. The first level, which includes sensor nodes, is responsible for collecting application data, monitoring the behavior of neighboring nodes, and some responding to intrusions locally (e.g. by isolating relevant nodes). The second level is the coordinator's level and is responsible for aggregating the application

data from the sensor nodes nearby and monitoring the behavior of the network or individual nodes. Identification of intrusions also will be done at this level by analyzing the aggregated data. Finally the intrusion reaction engine will react to the intrusions like done in the first level. Level three of the architecture detects intrusions by analyzing the application data from the coordinators. Similar to the access point level the base station level also has an monitoring and identification engine and will react to the intrusions which are detected at this point.

As described above, the functions of sensing, computation, and data delivery may be distributed across the tiers, with the lowest tier performing all sensing, the middle tier performing all computation, and the top tier performing all data delivery. Alternatively, each layer can perform a specialized role in computation.

8 Current Intrusion Detection Solutions for WSN

In this section we review some of the systems and algorithms which have been proposed for intrusion detection in WSNs. Some general approaches are presented as well as the algorithms which are based on Markov model. Some other solutions utilize mobile agents in order to detect and respond to intrusions.

8.1 General Approaches

Silva et al. [6], propose a decentralized intrusion detection for WSNs. Function of the IDS component is loaded into some nodes called "monitor" nodes. The detection system is specification-based, since the WSN may vary depending on the application goal. When deploying the sensor network, monitor nodes are distributed all over the network in a way that every node is covered by at least one monitor node. Their algorithm consists of three phases: in phase one which is data acquisition phase, messages are collected in a promiscuous mode and the important information is filtered before being stored for subsequent analysis. In the processing phase, the intrusion detection rules are applied to the stored data. Finally last phase or intrusion detection phase will determine if an intrusion detection is raised. The architecture of a monitor node is shown in figure 2. The IDS component of this node has three modules each one being responsible for a phase.

Du et al. [9] propose a general localization anomaly Detection (LAD) scheme. They consider the fact that some anomalies happen in the process

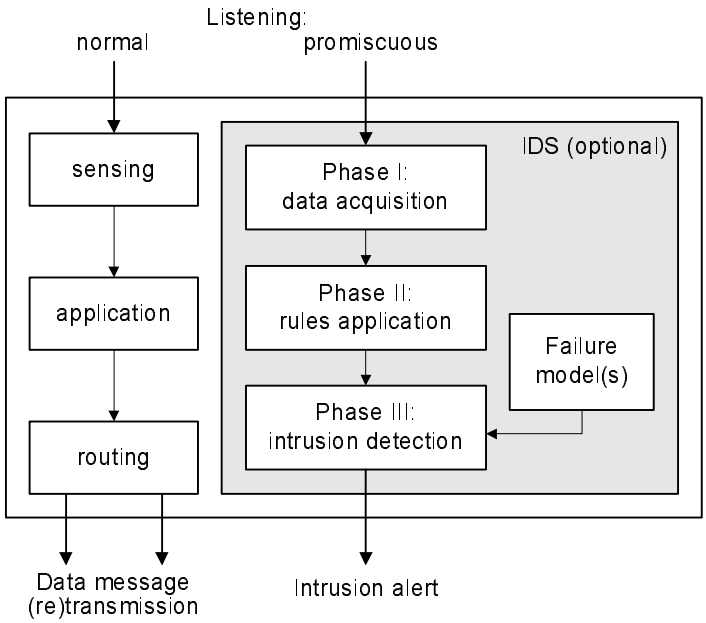

Figure 2: The architecture of a monitor node, adapted from [6].

of location discovery (localization). For instance deploying Global Positioning System (GPS) in every sensor, in order to determine location of the sensors, is costly. A number of solutions consider deploying GPS to just a few numbers of nodes in the network. The remaining nodes will verify their location using the location of sensors with GPS. We can see that this approach may result in localization anomalies by adversaries. The proposed scheme (LAD), takes advantage of the deployment knowledge and the group membership of its neighbors, and uses such knowledge to find out whether the estimated location is consistent with its observations. If they are inconsistent, LAD will report an anomaly. They formulate the problem as an anomaly intrusion detection problem, and introduce a localization anomaly detection phase after the localization phase. In the localization phase, sensors derive their locations. Then in the detection phase, sensors verify whether the derived locations are correct or not. A failure of the verification indicates an anomaly.

Mittal and Vigne [18] describe a signature-based intrusion detection technique which is for detecting routing-based attacks. Detecting these kinds of attacks is difficult because malicious routing behavior can be identified only in specific network locations. They use the characteristics of the Routing Information protocol (RIP), the network topology, and the positioning of the intrusion detection sensors to automatically determine both the signature configuration of the sensors and the messages that the sensors have to exchange to detect attacks against the routing infrastructure. The approach uses a set of sensors that analyze routing traffic in different locations within a network. An algorithm to automatically generate both the detection signatures and the inter-sensor messages needed to verify the state of the routing infrastructure has been devised for the case of the RIP distance-vector routing protocol.

In another work ([20]), intrusion detection functions are distributed to all the nodes in the network. The authors introduce a novel anomaly-based intrusion detection method for wireless sensor networks suited to their simple and resource-limited nature. This detection-based security scheme, which is for large scale sensor networks, exploits network stability in its neighborhood information. In many attacks against sensor networks, the first step for an attacker is to establish itself as a legitimate node within the network. If each node can build a simple statistical model of its neighbors behavior, these statistics can later be used to detect changes in them. The authors have shown that, by looking at a relatively small number of received packet features, a node can effectively identify an intruder impersonating a

legitimate neighbor.

8.2 Markov-Based Approaches

Doumit and Agrawal [8] propose an anomaly approach based on self-organized criticality (SOC) which is meant to link the multitude of complex phenomena observed in nature to simplistic physical laws and or one underlying process. Hidden Markov models are used to detect data inconsistencies. This approach is developed based on the structure of naturally occurring events. With the acquired knowledge derived from the self-organized criticality aspect of the deployment region, a hidden Markov model is then applied. The proposed approach lets sensor network adapt to the norm of the dynamics in its natural surrounding so that any unusual activities can be singled out. The work is focused on the fact that sensor nodes in WSNs are limited in resource and tries to minimize the resource consumption.

A new technique for handling security in WSNs is presented by Agah et al. [1]. They formulate the attack-defense problem by game theory and use Markov Decision Process to predict the most vulnerable sensor nodes. Their approach formulates attack-defense problem as a two-player, nonzero-sum, non-cooperative game between an attacker and a sensor network. In a non cooperative game unlike cooperative ones, no outside authority assures that players stick to the same predetermined rules, and binding agreements are not feasible. Each player (attacker and sensor network) tries to maximize its own payoff. Sensor network tries to defend the sensor nodes against intrusions. The algorithm is nonzero-sum in the sense that the increase in one players payoff implies the decrease in the other players payoff. The work shows that this game achieves Nash equilibrium and thus leading to a defense strategy from the network. Then, it uses Markov Decision Process to predict the most vulnerable sensor node.

8.3 Mobile Agent Utilization

One solution to perform distributed intrusion detection is by using mobile agent technology [15]. Agents can be seen as guards which protect a network by moving from host to host and performing random sampling. Instead of monitoring each host at any time, agents only visit machines from time to time to conduct their examinations. When any anomaly is detected, a more comprehensive search is initiated. Although the idea of patrolling guards seems appealing at first, this approach has the disadvantage of leaving hosts

Table 1: Classification of Different Solutions Based on Detection Technique

Detection Technique	Signature-based	Anomaly-based	Specification-based
Silva et al. [6]			X
Du et al. [9]		X	
Mittal et al. [18]	X		
Onat et al. [20]		X	
Doumit et al. [8]		X	
Kachirski et al. [13]		X	

vulnerable while no agents are present. On the other hand, random sampling definitely reduces the average computational load at each machine.

Kachirski and Guha [13] have proposed a distributed intrusion detection based on mobile agent technology. By efficiently merging audit data from multiple network sensors, their scheme analyzes the entire network for intrusions at multiple levels. There are three major agent categories: monitoring, decision-making, and action agents. Some are present on all mobile hosts, while others are distributed to only selected groups of nodes. The monitoring agents look for suspicious activities on the host node. If some anomalous activity is detected, the node is reported to the decision agent of the same cluster. The decision agent, then based on these reports, will decide weather the node has been compromised. When a certain level of threat is reached for the node in question, the decision agent dispatches a command that an action must be undertaken by local agents on the node.

Mobile agents introduce some advantages such as, reducing network load, overcoming network latency and scalability. On the other hand they may also result in some problems like, securing the agent itself and huge amount of code size.

Table 1 is a presentation of different solutions which are classified based on the detection technique used.

9 Conclusion

Research in intrusion detection has been conducted for the past twenty years, however, its application to wireless sensor networks is fairly recent. We have argued that any secure network will have vulnerability that an advisory can

exploit. This is specially true for WSN. Intrusion detection can complement intrusion prevention techniques to improve the network security. A number of research efforts concentrated on developing solutions for intrusion detection in WSNs in order to adapt with special characteristics of these kind of networks. Current solutions suggest distributed and cooperative intrusion detection and try to minimize false positives. Farther research efforts are needed to explore new methods to detect attacks against WSNs.

References

[1] A. Agah, S. K. Das, K. Basu, and M. Asadi. A non-cooperative game approach for intrusion detection in sensor networks. In *Third IEEE International Symposium on Network Computing and Applications*, pages 343–346, 2004.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. In *IEEE Communication Magazine 40 (8).*, 2002.

[3] F. Anjum, D. Subhadrabandhu, and S. Sarkar. Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols. In *Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida*, 2003.

[4] M. Bishop. *Computer Security: Art and Science*. Addison Wesley, Pearson Education, Inc., Boston, 2004.

[5] P. Brutch and C. Ko. Challenges in intrusion detection for wireless adhoc networks. In *SAINT: Symposium on Applications and the Internet*, pages 368–373, 2003.

[6] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong. Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 16–23, 2005.

[7] J. R. Douceur. The sybil attack. In *International Workshop on Peer-to-Peer Systems*, pages 251–260, 2002.

[8] S. S. Doumit and D. P. Agrawal. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks.

In *MILCOM: IEEE Military Communications Conference*, pages 609–614, 2003.

[9] W. Du, L. Fang, and P. Ning. Lad: Localization anomaly detection for wireless sensor networks. In *IPDPS: 19th IEEE International Parallel and Distributed Processing Symposium*, 2005.

[10] F. Hu and N. K. Sharma. Security considerations in ad hoc sensor networks. *Ad Hoc Networks*, 3(1):69–89, 2005.

[11] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *SASN: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, 2003.

[12] IEEE. Standard for part 15.4: Wireless MAC and PHY specifications for low rate WPAN. IEEE Std 802.15.4, IEEE, New York, NY, Oct. 2003.

[13] O. Kachirski and R. K. Guha. Effective intrusion detection using multiple sensors in wireless ad hoc networks. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, pages 57–65, 2003.

[14] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, May 2003.

[15] C. Kruegel. Applying mobile agent technology to intrusion detection. In *Distributed Systems Group, Technical University of Vienna*, 2002.

[16] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher. *Internet Denial of Service: Attack and Defense Mechanisms.* Prentice Hall, 2005.

[17] A. Mishra, K. Nadkarni, and A. Patcha. Intrusion Detection in Wireless Ad Hoc Networks. *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 48–60, February 2004.

[18] V. Mittal and G. Vigna. Sensor-based intrusion detection for intra-domain distance-vector routing. In *ACM Conference on Computer and Communications Security*, pages 127–137, 2002.

[19] Y. Okazaki, I. Sato, and S. Goto. A new intrusion detection method based on process profiling. In *SAINT: Symposium on Applications and the Internet*, pages 82–91, 2002.

[20] I. Onat and A. Miri. An intrusion detection system for wireless sensor networks. In *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, pages 253–259, 2005.

[21] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, 2004.

[22] R. Roman, J. Zhou, and J. Lopez. Applying Intrusion Detection Systems to Wireless Sensor Networks. In *Proc. CCNC 2006*, pp. 640–644.

[23] http://www.snort.org, Date visited: April,17,2006.

[24] W. Stallings. *Wireless Communications and Networks*. Prentice Hall, Upper Saddle River, NJ, 2002.

[25] D. Subhadrabandhu, S. Sarkar, and F. Anjum. Rida: Robust intrusion detection in ad hoc networks. In *Proceedings of The 4th International IFIP-TC6 Networking Conference*, pages 1069–1082, 2005.

[26] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.

[27] D. Xiao, C. Chen, and G. Chen. Intrusion detection based security architecture for wireless sensor networks. *IEEE International Symposium on Communications and Information Technology*, 2:1412–1415, 2005.

[28] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 275–283. ACM Press, 2000.

[29] Y. Zhang, W. Lee, and Y.-A HUang. Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks*, Vol. 9, pp. 545-556, 2003.