Wireless Sensor Network Security
J. Lopez and J. Zhou (Eds.)
IOS Press, 2008

Intrusion Detection Techniques in Sensor Networks

Aikaterini Mitrokotsa
Department of Informatics, University of Piraeus
80 Karaoli & Dimitriou Str. Piraeus, 18534, Greece
mitrokat@unipi.gr

A. Karygiannis
NIST
100 Bureau Drive, MS 8930, Gaithersburg,, MD, 20899, USA
karygiannis@nist.gov

1. Introduction

Research has been conducted in wired network Intrusion Detection Systems (IDS) for over 25 years. Although there is ongoing research in wired IDS techniques, it is considered a mature technology. Wireless area networks and personal area networks have been the focus of recent research, as they represent new risks and security challenges. Mobile Ad Hoc Networks (MANETs) have further challenged researchers to develop IDS techniques in an even more challenging environment. The promise of wireless sensor network technology to provide cost-effective monitoring of critical applications ranging from industrial control to border monitoring necessitates new research in the area of wireless sensor network IDS. The unattended nature and the inherent computational and communication limitations of sensor networks make them vulnerable to a broad range of attacks. Given the relative infancy of this new technology, the limited documented cases of actual sensor network attacks, the lack of publicly available network traces of sensor network attacks, most experience in this area is limited to simulations or laboratory emulations, with few approaches having been vetted in the field. This chapter outlines the unique challenges of wireless sensor network IDS and provides a survey of solutions proposed in the research literature.

2. Wireless Sensor Network IDS Challenges

Intrusion detection in wireless sensor networks presents a number of new and significant challenges not faced by wired, IEEE 802.11-based wireless, or even mobile ad hoc networks (MANETs). Although, previous research in IDS in these networks can serve as stepping stones for developing IDS techniques in wireless sensor networks, many of the techniques are not applicable due to the nature of the resource-constrained environment in which they will be deployed. In a typical wired network an adversary can launch an attack to compromise the network security perimeter from any other interconnected computer in the world. The adversary may use various techniques to conceal their attempts as well as their virtual and physical identity. A typical IEEE 802.11 wireless network in infrastructure mode presents new security challenges to the network administrator because communication between the access point and the clients is broadcast, and unlike the wired network, an eavesdropper does not need to have access to the wired network infrastructure to capture this traffic. On the other hand, the eavesdropper must be physically present and within the wireless transmission range to eavesdrop. This limits the number of potential attackers from anyone in the world with Internet access, to anyone sufficiently motivated that is within the physical transmission range and is willing to assume some risk of being physically identified. The goal of the attacker of the wired network is to compromise the network, to gain unauthorized access to information stored on network devices, and possibly to use the network resources to launch other attacks. The goal of the attacker in the IEEE 802.11 wireless networks is similar to those of the attacker of a wired network or may simply be the theft of service in the form of Internet connectivity. The goal of the attacker in a sensor network may be to either disrupt the operation of the sensor network, to provide false information to the sensor network application by providing incorrect data, or to gain unauthorized access to the sensor network data which is inevitably stored in the base station and forwarded to other computing devices. The base station is an attractive target for attack because it contains almost all the sensor data. Fortunately, the base station is typically more powerful than the sensor nodes themselves and can make use of existing mature security countermeasures that are not yet available to the sensor nodes. Although the universe of potential attackers of a particular sensor network is less than that of potential attackers of a computer on the Internet, an adversary of a sensor network can be assumed to be more motivated and less opportunistic. An attacker on the Internet might use attack scripts to attack any vulnerable network, while a sensor network is more likely to be the focus of a goal-oriented attack. The attacker of the sensor network has risen above the threshold of the remote attack using “kiddie scripts” by taking greater physical risks.

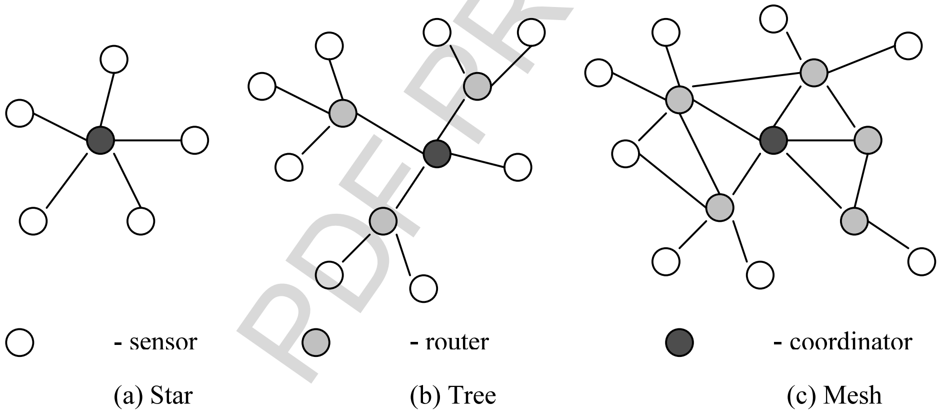
Many scenarios have been proposed in the research literature citing the ease of deployment of sensor networks, many metrology experts, however, would argue that the placement of sensor nodes is highly dependant on the application and that test measurements are essential whenever possible to ensure the quality and usefulness of the data collected. If the sensors can be physically placed by an organization, it stands to reason that the distribution of the keying material can also be restricted to an authorized user that has physical access to the sensor nodes during the deployment stage. The ability to restrict the distribution of keying material only to authorized users can serve as an advantage to those responsible for the security of the sensor network. Physical access to the sensors to distribute keying material makes the sensors less vulnerable to networks attacks, while the unattended deployment of the sensors makes them more vulnerable to physical attacks.

Like all wireless technologies, sensor network communication is susceptible to jamming. Although jamming is difficult to prevent, it is more easily detected and located than a Denial of Service (DoS) attack on the wired Internet. DoS attacks on the Internet may be launched by botnets and carried out by compromised machines running zombie processes in the background unbeknownst to the owner of the machine, thus the risk for physical identification and apprehension of the attacker is reduced.

Jamming a sensor network requires the adversary to place the jamming equipment within the transmission range of the sensor network, thereby exposing the adversary to a greater risk of physical identification and apprehension.

Wireless sensor networks IDS's face different challenges and have more constrained resources with which to counter these threats. The selection of which IDS technique to use depends on a number of factors. These factors include:

- **Network Topology.** Although many sensor networks are described as self-organizing, what this really means is that the sensors will discover the route to the base station on their own. The physical placement of the sensors themselves must ensure a minimum level of connectivity and in many cases sufficient redundancy. The placement of the sensors requires careful study and the selection of the sensor location is not as arbitrary as some of the literature may suggest. If the sensor network topology provides for redundancy of measurements, then it also provides the opportunity for one sensor to validate the measurements reported by another sensor. Just as the base station provides a rich target for an adversary, so do the sensor nodes that are closest to the base station as more data collected from the edge of the network passes through these sensors. We note that a mesh topology is more resilient to individual node failure or compromise. If the sensor network topology is tree-like, individual nodes are likely to be vertex-cuts of the sensor network and their failure or compromise could lead to a disconnected network.



(a) Star (b) Tree (c) Mesh

Figure 1. Sensor Network Architectures.

- **Mobile vs. Stationary.** In a sensor network both the sensors and base station may be mobile, both the sensors and base station may be fixed or stationary, or the network may be some combination of the two. In the case of mobile sensors, the sensors may be attached to shipping containers to monitor the condition of the cargo while in transit and report the measurements to different base stations along their journey. These sensors may be queried by an authorized base station. In this case, there may be limited physical controls to restrict access to the sensor and the sensor may be unattended for long periods of time. Base stations may be mobile, for example, in the case of a utility company a base station or sensor reader may query fixed sensors as the utility company vehicle travels through a densely populated area. In the case of the stationary sensor, monitoring water consumption for example, physical controls may be used to protect the sensor hardware. The base station may be physically secured in the utility company vehicle. In this case the main threat and financial concern would be someone tampering with the integrity of the sensor readings.

- **Open vs. Closed Sensor Networks.** A closed network is one in which participation is limited to nodes under the same administrative domain, while an open network allows any node, sometimes with prior authorization, to join on an ad hoc basis. A closed network allows for more administrative control over each individual node, while an open network must support standards-based protocols and interoperability in order to allow nodes without any prior security associations to join the network. If membership in the closed network requires the possession of a shared key or identity certificates, then the sensor nodes must have cryptographic support and require online security services such as certificate authorities in order to dynamically join the network. These higher level security services may also be targets of attack in order to disrupt the sensor network operation.

- **Physically Accessible or Inaccessible.** An attack on the sensor network communication protocols or simply eavesdropping on sensor network communication requires physical proximity to the sensor network. Although eavesdropping may be confined to sensor communication operating ranges, jamming is a much less selective technique that depends on the power of the jamming source. If an adversary has physical access to the sensors, then one could assume that the adversary can place their own sensor, depending on the application, in the same location. If the sensors are complex or cost-prohibitive to replicate then naturally the adversary would want to target the base station or the sensor communication. Clearly, each sensor application needs to be analyzed in order to quantify the risks and to select the appropriate countermeasures. Biochemical sensors, for example, are typically more complex, costly, and larger than temperature, pressure, and accelerometer sensors. The more costly the sensor the less likely the availability of redundant measurements or the overlapping of monitored areas.

- **Application Domain.** Typical network-based and host-based IDS may make use of log and audit files to detect intrusions. Although these techniques may not always be available to sensor networks, sensor networks can also take advantage of application-level IDS for each particular domain. For example, a faulty sensor that is reporting physical measurements that are inconsistent with other physical phenomena can be detected by analyzing the data at the application level. These applications would be similar to system diagnosis techniques that analyze the collected data to detect and diagnose potentially faulty sensors. The problem of differentiating between a faulty sensor and a malicious sensor is very difficult. A sensor may be experiencing a physical failure and report erroneous data, an intruder may be tampering with the sensor hardware, or the data may be modified on the sensor or while in transit.

- **Critical or Non-Critical Application.** The necessity for the collection of real-time data for critical applications will also have an impact on the types of countermeasures that can be used. An industrial application, for example, would require real-time detection and response to a potentially dangerous situation. A long-term environmental monitoring application may not require an immediate response. The environmental monitoring application may employ sensors that are unattended for long periods of time, while the industrial application may have the sensors confined within the physical perimeter of a factory and thus face a different threat environment. Sensor networks may often be deployed in critical applications such as biochemical agent monitoring in urban areas or transportation systems. In the case of biochemical agent sensor networks, video sensors are often used to help system operators respond to critical events. In the case of a biochemical sensor, the system operators are faced with the decision of sending a team of experts to the location in special suits to protect first responders against hazardous materials and as a result raise the risk of public panic. In a fire monitoring sensor network, visual corroboration can be used to eliminate costly responses to false-positives. Sensor networks can be comprised of nodes of varying degrees of complexity, network connectivity, and cost depending on the application. Moreover, depending on the criticality of the application, sensor networks are likely to be deployed in conjunction with other technologies and human processes to ensure the robustness of the monitoring and control processes.

- **Hazardous or Non-hazardous Environment**. If the sensor network is deployed in a non-hostile environment we must also consider the physical threats faced by the sensor network. These threats can include an adversary tampering with the exposed sensor circuitry, physical attacks to extract the keying material from the sensor node, and placing new or cloned sensors within the network to provide false data. If sensors are deployed in hazardous environments, then it would stand to reason that the sensors themselves are less vulnerable to physical attacks, but they are more likely to be the target of either denial of service or eavesdropping. These environments also make the base station, from which the data is ultimately to be collected, a more attractive target. If sensors are deployed in non-hazardous environments and no physical countermeasures are available to prevent physical tampering with the devices, then the sensors themselves and the sensor network application must be able to detect tampering. Tamper-resistant and tamper-evident technologies can be employed to help detect and diagnose physical attacks against the sensor network.

- **Routing Algorithms.** Support for more sophisticated routing algorithms provides the opportunity to use network traffic analysis to detect malicious activity. Sensor network protocols, however, have been designed with simplicity and power conservation as their main goals. The most common sensor routing technologies are ZigBee, TinyOS, and IEEE 802.15.4. TinyOS is an event based operating environment designed for sensor networks. TinyOS is designed to support two of the most basic protocols used in sensor networks: dissemination and collection. Dissemination reliably delivers small data items to every node in a network, while collection builds a routing tree rooted at a sink node. Together, these two technologies enable a wide range of data collection applications. The Zigbee standards define the network, security and application software layers for wireless sensor networks. The lowest level of the communications stack defined by Zigbee is the networking level. Zigbee is not a MAC protocol, an operating system, or a hardware platform. The Zigbee standards are not open source and are only available to Zigbee Alliance members. The IEEE 802.15.4 standard defines a MAC and PHY layer for wireless sensor networks (http://www.ieee802.org/15/pub/TG4.html). The IEEE 80.15.4 standard has 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz I and one channel in the 868MHz band. The IEEE 802.15.5 standard has CSMA-CA channel access, supports data rates of 250 kbps, 40 kbps, and 20 kbps, provides automatic network establishment by the coordinator, and incorporates power management to ensure low power consumption. The Zigbee standards assume an underlying 802.15.4 layer.

- **Cryptographic Support.** Support for cryptographic protocols allows sensor networks to address access control, message integrity, and message confidentiality requirements. Public key cryptography is prohibitively expensive for sensor networks in terms of computation and energy consumption. It must be used sparingly or not at all. Developing security mechanisms using efficient symmetric key cryptography is more promising, but packet overhead is still a significant problem. Symmetric key encryption and authentication mechanisms for conventional networks typically require at least 16 bytes of overhead per packet. This is almost half the current packet length used in sensor networks. TinySec is a link layer encryption mechanism for devices running TinyOS. The core of TinySec is a block cipher and keying mechanism that is coupled with the Berkeley TinyOS radio stack. TinySec uses a single, symmetric key that is shared among a collection of sensor network nodes. Before transmitting a packet, each node first encrypts the data and applies a Message Authentication Code (MAC), a cryptographically strong hash to protect the data integrity. The receiver verifies that the packet was not modified in transit using the MAC and then deciphers the message. TinySec supports three main security requirements: access control, integrity, and confidentiality. TinyECC is an Elliptic Curve Cryptography (ECC) implementation for TinyOS. TinyECC supports all elliptic curve operations, including point addition, point doubling and scalar point multiplication. In addition to the basic elliptic curve operations, TinyECC supports ECDSA operations (signature generation and verification). TinyECC has been tested on both MICAz, TelosB and Imote2. TinKeyMan provides an implementation for pairwise key establishment in wireless sensor networks using the polynomial pool-based key predistribution scheme.

- **Sensor Network as Part of a Larger Network.** The vast amount of information collected by sensor networks would prove far more valuable if it could be shared with authorized users connected to other wired or wireless networks. In open networks, for example, a mobile base station could traverse a city gathering sensor data from various data providers. Each sensor network deployed by each organization will likely be under a different administrative domain, support different security protocols, and employ different access control policies. For example, a first responder could run an application on a wireless handheld device that would collect data from different sensor networks deployed by the Centers for Disease Control and Prevention (CDC), the National Oceanic and Atmospheric Administration (NOAA), and the New York Metropolitan Transportation

Authority (MTA). The handheld device can be part of a MANET, and the application can help the first responder best react to an emergency and help commuters evacuate a certain area, for example, by taking traffic patterns and weather conditions into consideration. Clearly, this example can be extended to support countless applications that need to access sensor data over heterogeneous wired and wireless networks. To enable these types of applications, the consumer of the data must be able to locate the producer of the data, and then subsequently gain authorized access to this data by providing the appropriate credentials. The producers of the data must be able to advertise the services they offer and be able to authenticate the consumers of this data. Some of the sensor data collected by the sensor base station may be very useful, but not confidential, such as the temperature or wind speed in a particular location; other sensor data may be confidential and require certain privileges to access. Thus, the sensor base station must have security policies in place to provide access control to its data. If the sensor network base station can serve as a gateway to a wider network, then the base station must employ security mechanisms that are deployed in conventional wired and wireless networks.

- **Sensor Network Support Infrastructure.** The data collected by the sensors can be targeted while on the sensors themselves, during intra-sensor communication, during sensor-to-base station communication, while on the base station, while the base station is transferring the sensor data back to a data repository over wireless or wired links. A number of other security services may be used to support the sensor network, such as service directories and certificate authorities; all of which could be the target of an attack to disrupt the sensor network operation. Countermeasures for security risks outside the sensor network are well documented and should be used by the base station assuming the base station is acting as a gateway to a broader network.

3. Wireless Sensor Networks Attacks

In order to better understand the attacks an IDS must be able to prevent, counter, detect, and respond to, this section provides a brief overview of sensor network attacks. We note that an attacker may be equipped with either malicious nodes or more sophisticated computing machinery like a laptop or signal generator and signal processing equipment, may be an inside attacker or an outside attacker, or may be a passive or an active attacker. Most trust models assume that the base station is trustworthy as long as it is available. Given the great value of the base station one can argue that it is more likely to be attacked than a sensor especially since it is also more likely to have network connectivity through a wired or wireless gateway.

Sensor networks are susceptible to attacks starting from the physical layer and going all the way up the stack to the application layer. Roosta et. al. [2] provide the following classification of sensor network attacks:

- *Physical Tampering.* Physical attacks can include probing techniques on the sensor circuitry or side channel attacks.

- *Software Attacks*. Software attacks attempt to modify code and exploit software implementation vulnerabilities.

- *Physical Layer Attacks*. Physical layer attacks take advantage of the wireless broadcast medium to simply jam the radio frequency so that no useful communication can occur.

- *Link Layer Attacks*. Link layer attacks can cause excessive collisions in the packet transmission, exhaust the battery's capacity as the result of unnecessary retransmissions, or not adhering to the Carrier Sense Multiple Access (CSMA) protocol and monopolizing the wireless channel.

- *Network Layer and Routing Layer Attacks*. Network and routing layer attacks include: black holes attacks, wormhole attacks, spoofed, altered, and replayed packets, selective forwarding, sinkhole attacks, and acknowledgement spoofing.

- *Transport Layer Attacks*. Transport layer attacks include flooding attacks and desynchronization attacks. The flooding attack aims to exhaust the target's resources by sending an excessive amount of communication requests, while the desynchronization attack alters the sequence numbers of the packets in order to disrupt the communication protocol.

- *Traffic Analysis Attacks*. Traffic analysis attacks allow an adversary to deduce information about the network topology and the location of the base station by monitoring traffic transmission patterns. Once the topology of the network is known, the attacker can selectively target nodes to attack.

- *Key Management Protocol Attacks*. Key management protocol attacks observe the nodes during the discovery process of the shared keys and try to break the cryptographic techniques using more powerful computing devices.

- *Sybil Attack*. Sybil attacks occur when a sensor node or base station assumes multiple identities by changing its MAC and IP address or other identifying information.

4. Wireless Sensor Network Intrusion Detection

Conventional intrusion detection techniques are divided into two main categories: misuse detection and anomaly detection. Misuse detection, or signature-based detection, uses *a priori* knowledge of intrusions and tries to detect attacks by comparing the observed behavior with known attack patterns (signatures). Although misuse detection systems are very accurate in revealing known attacks without many false alarms, their basic disadvantage is that attack mechanisms are continuously evolving, which leads to the need for an up-to-date knowledge base. Thus, misuse detection systems are unable to detect attacks not included in the knowledge base. Misuse detection techniques in resource-constrained environments require additional research in the efficient storage and updating of attack signatures in order to be a viable solution in sensor networks.

Anomaly detection systems use established normal profiles and attempt to track deviations from normal behavior in order to detect anomalies or possible intrusions. If the normal behavior is accurately characterized then anomaly detection has the advantage of being able to discover previously unknown attacks. Anomaly detection systems, however, are not extensively used in commercial systems due their high false alarm rate. Sensor networks are typically private networks and there may be no incentive to share attack signatures. Unlike public networks like the Internet, there is no precedent for sharing of sensor attack signatures and little is known of any actual sensor network attacks. Most attacks are postulated and the defenses against them are confined to simulations. Organizations deploying sensor networks may be reluctant to share the details of sensor network intrusions for the same privacy and security reasons that most organizations are reluctant to disclose details about wired network intrusions. Furthermore, anomalies are not easily distinguishable from localized, incomplete and possibly outdated information or simple sensor failures and malfunctions.

4.1 Intrusion Detection in Sensor Networks

Intrusion detection techniques developed for wired networks cannot easily be deployed in sensor networks due to the differences between the two types of networks. First of all, sensor networks do not rely on any fixed infrastructure. Thus, compared to wired networks where traffic can be monitored in gateways, routers and switches, sensor networks and wireless ad hoc networks in general, lack traffic management points where real-time traffic monitoring can be performed. In addition, audit data collection is limited by the radio range of the devices. Furthermore, differentiating between malicious network activity and spurious, but typical problems associated with an ad hoc networking environments is a challenging task. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection. The loss or capture of unattended sensors and personal computing devices may allow for a malicious node to obtain legitimate credentials and launch more serious attacks. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an ad hoc network does not have these types of network elements where the IDS can collect audit data for the entire network. A wired network under a single administrative domain allows for discovery, repair, response, and forensics of suspicious nodes. A MANET is most likely not under a single administrative domain, making it difficult to perform any kind of centralized management or control. Network traffic can be monitored on a wired network segment, but ad hoc nodes or sensors can only monitor network traffic within their observable radio transmission range [31].

Although, many intrusion detection algorithms have recently been proposed for wireless ad hoc networks, neither intrusion prevention nor intrusion detection solutions for wireless ad hoc networks can be directly applied to wireless sensor networks. We outline some of the important differences between wireless ad hoc networks and sensor networks that seriously affect security requirements.

In a sensor network, every node has an asymmetric broadcast communication pattern. Each node sends data and receives control packets from the base station, which is usually managed by a human. An important advantage of this forwarding structure is its immunity against many elaborate routing attacks [3]. Furthermore, the computing and power resources are even more constrained in sensor nodes than in ad hoc nodes. Thus, resource depletion attacks may be launched more easily in sensor networks. Sensor nodes in most applications are stationary. Thus, the routing overhead is decreased. Moreover, sensor networks are application-oriented, with specific characteristics depending on the target application. Thus, both hardware modules and communication/configuration protocols are highly specialized, making it difficult to define “usual” or “expected” behavior. Additionally, since sensor nodes are subject to more severe resource constraints than ad hoc nodes they are more prone to failure and disappearance from the network [4]. Also sensor nodes may not have global identification (ID) due to the large amount of overhead, the large number of sensors and the lack of Domain Name System (DNS) for sensor nodes unless they support a network stack or have an Internet Protocol (IP) address.

These differences have a direct impact on the way that intrusion detection can be performed in sensor networks. Having an active full-powered agent inside every node [4] is can be very resource-intensive. The memory constraints of sensor nodes makes, for example, make the creation and possible recovery of a detection logfile extremely difficult.

4.1.1 Requirements for Intrusion Detection in Sensor Networks

The design of an IDS for sensor networks should consider the following requirements and constraints [5]:

- An IDS for sensor networks should be based on a distributed architecture applied not only for the data collection, but also for the execution of the intrusion detection algorithm and the alarm correlation. However, we should keep in mind that any collaboration or and trust-building techniques should keep the demands on resources at a minimum..

- Since sensor networks face resource constraints, the IDS system should conserve as much power as possible [6]. Furthermore, considering the fact that the majority of the power consumption comes from the communication interface and not the computation itself, the IDS techniques should not have an inordinate amount of communication overhead.

- Furthermore, considering the resource constraints of sensor devices, the locations where packets are sniffed and analyzed should be minimized while balancing any negative impact on the efficiency of the IDS.

- The lack of centralized points (apart from the base station) in sensor networks that could be used for global collection of audit data, render the localized collection of audit data a necessity.

- Since sensor nodes are highly vulnerable, no node can be assumed to be secure and cooperative algorithms should not consider any node as fully trusted.

- An IDS must be able to safeguard itself against malicious attackers. The possible compromise of a monitoring node should not have a negative impact on the normal operation of legitimate nodes.

- In order to minimize the impact of a possible intrusion in critical applications, it is important that an IDS for sensor networks to function in real time.

5. Sensor Network IDS Architectures

There are two basic sensor network architectures, *flat* and *hierarchical,* that specify how sensors are grouped and how sensor information is routed through the network. In flat architectures all sensor nodes have almost the same communication capabilities and resource constraints and the information is routed sensor by sensor. In hierarchical architectures, sensors are grouped into clusters. One of the member nodes is the "cluster head" and is responsible for management and routing tasks. A challenging research issue is the placement of the IDS modules in sensor networks in order to achieve efficient and effective intrusion detection. A number of placement strategies have been proposed. The following paragraphs describe the most important of those found in the research literature [7], as well as their advantages and disadvantages.

Promiscuous monitoring: A simple strategy would be to place IDS modules in every sensor node as illustrated in Figure 2 and to have each node operate in a promiscuous mode (always listening on the wireless interface). In this way, any malicious packet can be easily detected. However, because of the high overhead associated with this strategy, each participating node's ability to forward network traffic is severely reduced. Furthermore this IDS module placement strategy may lead to network traffic collisions and power consumption.

- **A node monitors only the packets that pass through it.** According to this placement strategy the IDS modules are also placed on every sensor node as illustrated in Figure 2, but only the packets that pass through each sensor node are used for the analysis. Thus, the IDS modules are placed on every sensor along the path from a source to a destination. This approach implies that each packet is analyzed multiple times leading to a waste of computational resources.

- **IDS modules on the base station.** Another possible strategy would be to place the IDS modules on the base station as illustrated in Figure 3. The base station can analyze all the traffic in the sensor network regardless of topology or routing changes and each packet is not processed multiple times. Nevertheless, although a packet is not processed many times, this placement strategy might overwhelm the base station leading to a large number of packets not being analyzed.

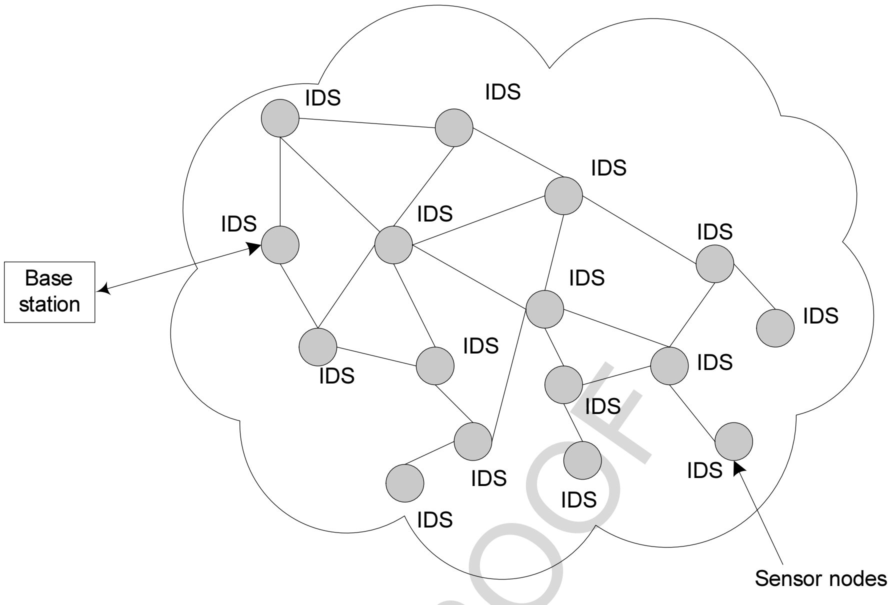


Figure 2. Distributed IDS architecture.

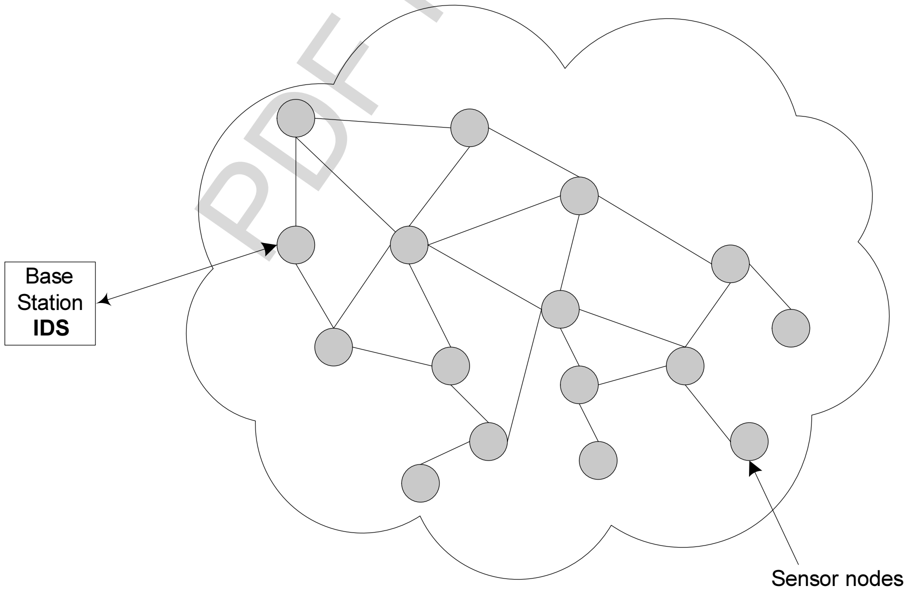


Figure 3. IDS module on the base station.

- **IDS modules on every neighbor of the base station.** In order to reduce the computational load on the base station, IDS modules can be placed on every neighbor of the base station. However, this architecture, cannot combat resource exhaustion attacks since flooding packets will only be dropped when they reach their destination.

- **IDS modules in "cluster heads".** An efficient solution for the placement of IDS modules would position the IDS monitors in such a way that all the packets would be inspected only once, in order to address the resource constraints of the sensor networks. Thus, the IDS modules could be placed in selected sensor nodes (Figure 4) that would be able to cover all the paths from every source node to the base station. In order to achieve this, the sensor network may be divided into clusters with each cluster having a cluster head. This placement strategy implies that every member node of a cluster should forward its data packets to the cluster head which correspondingly forwards them to the base station. However, this approach may lead to a high overhead since the member nodes do not select the shortest path, but instead have to forward their packets through the cluster head. This disadvantage may be limited if the hops between each member node and the cluster head are minimized.

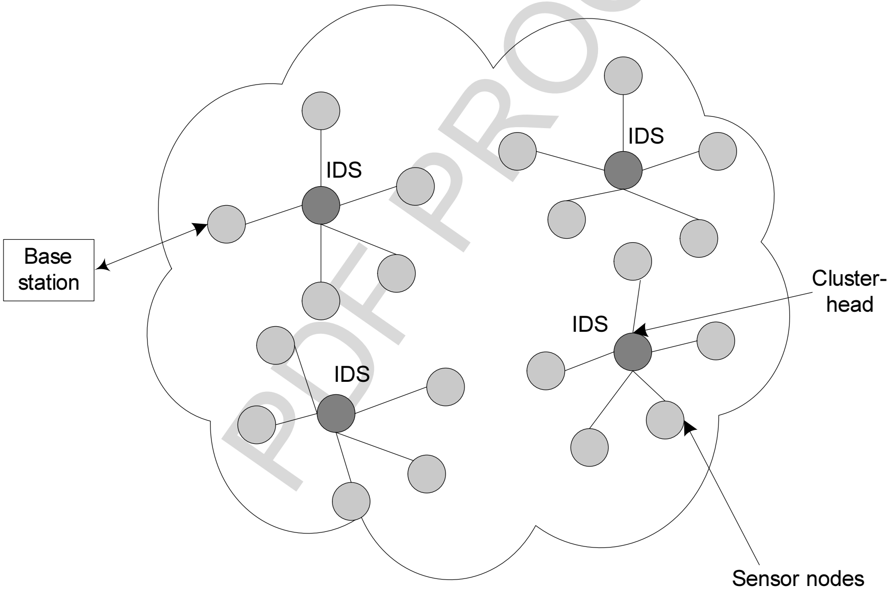


Figure 4. Cluster-based IDS architecture.

The placement of IDS modules is an active research field and many resource optimization approaches have been proposed. Anjum et. al. [7] use a minimum cut set to choose the minimum number of cluster heads. The IDS modules are placed on the nodes that belong to the cut set, but in order to minimize the communication overhead since now the packets do not take the shortest path to the base station, the concept of the minimum weighted dominating set is used. A distributed implementation to determine the minimum cut set is provided. Anjum et. al. have shown that the proposed algorithms perform well when compared to the random placement of IDS modules on sensor nodes. They also discuss the importance of cooperation amongst the defenders of sensor networks. Furthermore, the proposed approach is evaluated in the case of multiple colluding intruders. We note here that signature-based intrusion detection is assumed, thus; this approach does not address the problem of unknown attacks.

Techateerawat et. al. [8], investigate the accuracy of detecting attacks in sensor networks versus energy efficiency. They investigate new approaches to intrusion detection based on the layout and the selection of monitoring nodes. An analysis is presented based on the response of intrusion detection nodes, the number of required alert messages and the intrusion detection ability. The analysis includes variations in the size of clusters. They are based on a decision mechanism derived from Siraj et al. [9] which combines misuse and anomaly detection. The authors attempt to minimize the number of nodes where the IDS module will be deployed and investigate the following three strategies: core defense, boundary defense, and the distributed defense. According to the core defense the selected nodes are around a central point. In the boundary defense the selected nodes are along a boundary at the perimeter of the cluster. While in the distributed defense the nodes are selected according to a voting algorithm [10]. Their simulation results demonstrate that small clusters may present efficient performance with all defense strategies without significant differences in energy consumption. On the other hand, when the cluster size is large, distributed defense is very energy-intensive, while boundary and core defenses are more economical in energy use, but are vulnerable to insider attacks (from within the cluster).

Roman et. al. [4] propose a general architecture for applying IDS in static sensor networks and propose a *spontaneous watchdog* technique for optimally monitoring neighbor nodes. According to the proposed architecture, IDS agents are located on every node. Every node has an internal database that is used for storing security information collected by the node IDS agents. The IDS agents are divided into two parts, local agents and global agents. *Local agents* are responsible for monitoring the local activities and the packets sent and received by the sensor. Thus, they attempt to discover any attack that may affect the normal behavior of a sensor node by analyzing the local information. This analysis is carried out only when the sensor is active, thus the imposed overhead is low. *Global agents* are responsible for watching the communications of their immediate neighbors and may behave as watchdogs [11]. If all the global agents are activated and listen to their neighbors at the same time, this would be a highly costly operation, thus only a small subset of nodes watch the network communications at any given time.

The way global agents are activated depends on the routing architecture that a sensor network adopts. In hierarchical architectures, global agents are activated in every cluster, since the combination of all clusters covers the entire network. In flat architectures the selection of activated global agents is difficult since it is not possible to know what agents cover the network. Since clustering techniques add complexity and increased overhead for the creation and maintenance of the clusters, an alternative distributed solution, called spontaneous watchdogs approach is proposed. The spontaneous watchdog technique relies on the broadcast nature of sensor communications and takes advantage of high density sensor deployments. The main goal is to activate only one global agent per packet circulating in the network and is performed by algorithm that checks the destination of every packet.

6. Sensor Network IDS Approaches

IDS approaches proposed for safeguarding sensor networks can be classified into four distinct categories:

- IDS using routing protocols,
- IDS based on neighbor monitoring,
- IDS based on innovative techniques, and
- IDS based on fault tolerance.

6.1. IDS using Routing Protocols

Loo et. al. [12] and Bhuse and Gupta [13] describe two intrusion detection techniques for routing attacks in sensor networks. However, both proposed approaches are based on the assumption that routing protocols for ad hoc networks can also be applied to sensor networks [5]. The AODV (Ad hoc On-Demand Distance Vector) routing protocol is used by Loo et. al. [12], while DSDV and DSR (Dynamic Source Routing) protocols are used by Bhuse and Gupta [13]. Most commercially available sensors, however, do not support ad hoc routing algorithms such as these.

Loo et. al. [12] propose an intrusion detection scheme that uses a clustering algorithm and classifies anything that deviates from normal routing traffic patterns as abnormal traffic patterns. The proposed approach is based on a *fixed-width clustering* algorithm, which is highly effective for anomaly detection in Internet Protocol (IP) networks. It is based on anomaly detection thus; it is able to detect unknown attacks. The intrusion detection approach is based on a set of traffic features that could be used for the detection of a wide range of attacks. The proposed approach is based on distributed Local Intrusion detectors that rely solely on information extracted form each node’s routing tables. Thus, no communication between sensor nodes is required, an important advantage considering the scarce power resources of sensor networks. The limitation of this approach, however, is that ad hoc routing algorithms use routing tables, but many sensor nodes simply communicate with a parent or child node without being aware of which route packets may traverse to reach their final destination. The proposed approach is evaluated for three routing attacks: the *Periodic Route Error attack, Active Sinkhole attack, Passive Sinkhole attack.* Also this scheme proved to be very efficient for the detection of sinkhole attack, an attack with severe impact on sensor networks.

Bhuse et. al. [13] propose lightweight methods in order to perform intrusion detection in sensor networks. The proposed methods use existing system information such as neighbor lists, routing tables, sleep and wake up schedules etc., and attempt to detect the malicious behavior at multiple layers. Thus, if an attacker manages to escape detection at one layer, there are many opportunities to detect the malicious activity in the other layers. The detection methods at each layer are independent of each other and may be used in combination depending on the needs and the available resources.

6.2. IDS based on Neighbor Monitoring

Da Silva et. al. [6], Onat and Miri [3], Krontiris et. al. [5] and Hsin et. al [14] propose intrusion detection approaches that present some similarities to each other. In all these approaches some sensor nodes monitor their neighbors in order to detect possible intrusions. According to the proposed methods, the monitoring nodes select data from messages transmitted in their radio range and select related information including message fields. This data is used as input to the corresponding IDS. This is similar to the proposed watchdog techniques described in the MANET IDS research literature [11].

More specifically, Da Silva et. al. [6] propose a decentralized intrusion detection approach. According to this approach, the monitoring nodes watch their neighbors. If a sensor node changes, delays, replicates or simply keeps and does not forward the received messages as required, then the monitoring node records it as a failure and an indication of a possible intrusion. Thus, a monitoring node creates a history for each of its neighbors. If the number of failures detected by the monitoring node is greater than an expected value then an attack level is raised. In order to avoid a possible high false positive rate, a learning stage is introduced, during which a monitoring node does not consider any abnormal event until the average number of failures has settled. The evaluation of the proposed approach has been performed for three types of occasional network failures and eight types of intruder attacks. The occasional network failures are data alteration, message loss and message collision. The intruder attacks are message delay, repetition and wormhole, jamming, data alteration, message negligence, blackhole and selective forwarding.

The proposed intrusion detection approach by Onat et. al. [3] is based on the average packet arrival rate and the average received power level as representative features for each neighbor. Each node uses only the last *n* packets received from each neighbor and these packets are used for the calculation of statistics for each neighbor node. However, in both these proposed approaches [6], [3] the monitoring nodes do not collaborate and the buffer size plays a substantial role in the efficiency of the detection and the low false alarm rates [5].

Krontiris et. al. [5] propose a lightweight distributed intrusion detection approach for sensor networks based on specification-based detection,. According to the proposed approach, each sensor node hosts an IDS agent. The IDS agent performs network monitoring, decision making and response. During the network monitoring task, every sensor node monitors each immediate neighbor and collects audit data. During the decision-making task every node based on local audit data determines the existence of possible intrusions and forwards their conclusions to each immediate neighbor in order to make the final collective decision. The local detection engine applies the defined specifications about what is normal behavior and monitors audit data according to these constraints. The cooperation between neighboring nodes is performed by applying the majority vote rule in order to determine the existence of an attack. Furthermore, when an attack is detected the local response module is activated. Depending on the severity of the attack the response might be direct or indirect. The direct response excludes the suspect node from the routing paths and forces regeneration of cryptographic keys for the rest of the neighbors. The indirect response notifies the base station about the suspected behavior of the possible intruder and reduces the reputation of the link to that node so that gradually it will be characterized as unreliable. The proposed approach is evaluated against the blackhole attack and selective forwarding attacks. This approach is a bit antithetical to many sensor designs that try to keep the wireless interface off unless the sensor node must report data. We note that the wireless interface consumes much more power than the computing processor.

Hsin et. al. [14] propose a low overhead network health monitoring algorithm. This approach is relevant in the context of an IDS since the IDS must always be able to differentiate between malicious behavior and normal operational failures. Making this distinction in sensor networks is even more important because of the physical exposure of the sensors to environmental elements and physical attacks. They propose a distributed monitoring mechanism for wireless sensor networks which focuses on localized decision making and the minimization of false alarms by testing whether a group of sensor nodes are dead or alive. The proposed schema can be seen as a passive monitoring mechanism which notifies the control center only if it is highly confident that something is wrong. The basic principle of the proposed approach is based on neighbor monitoring. Each sensor sends its update messages only to its neighbors and every sensor monitors its neighbors. The monitoring is controlled by a timer associated with each neighbor. Thus, if a sensor has no communication with a neighbor for a pre-defined period of time, then the neighbor is assumed to be dead. By mutual monitoring between neighbors, the monitoring performed throughout the network and the control center has to monitor only a small subset of nodes. Furthermore, local decision making is performed since each node makes some decisions before communicating with the control center. Each node increases the confidence of its decisions by consulting each neighbor. The total amount of traffic sent to the control center is minimized by adopting a simple query-rejection or query confirmation procedure and minimal neighbor coordination. We should note here that the neighbor monitoring works only if every node is reachable from the control center.

C.C Su et. al. [15] propose an authentication-based intrusion detection and response approach for wireless sensor networks. Using an intrusion prevention mechanism they authenticate exchange control messages between sensor nodes. According to their intrusion detection approach different monitoring mechanisms are needed to monitor cluster heads and member nodes relative to their importance. Network members perform the monitoring of cluster-heads in turns. Thus, the monitoring time is reduced and member nodes conserve energy. The monitoring of member nodes is performed by cluster heads that have the authority to detect any misbehaving node and isolate the malicious node by broadcasting an encrypted alarm message. Energy conservation is achieved, since cluster-heads are used for monitoring instead of using all member nodes to monitor each other. Furthermore, the intrusion response of the proposed approach is activated only when the detection of alarm messages comes from at least X monitoring nodes that detect the misbehavior of the same cluster head. Thus, the proposed intrusion detection approach has the advantage of being tolerant of compromised nodes within a threshold in a cluster. However, a cluster head could isolate too many member nodes and this way to reduce its own security. In order to avoid such an event, the member nodes that monitor the cluster head should determine whether or not the cluster head should be changed depending on the number of monitoring nodes. Nevertheless, the proposed intrusion prevention mechanism does not allow new nodes to join the network and assumes that sensor nodes do not move.

6.3. IDS based on Innovative Techniques

Agah et. al. ([16], [17]) suggest that game theory can be applied to intrusion detection in sensor networks. They propose an approach for the prevention of DoS attacks in sensor networks based on a game theory approach. The prevention approach is formulated as a repeated game between an intrusion detector and the nodes of a sensor network. They propose a protocol based on game theory which is able to recognize the nodes that agree to forward packets, but fail to do so. The approach categorizes different nodes based upon their dynamically changing behavior and enforces cooperation among nodes. Any non-cooperative behavior is punished. The intrusion detector situated at the base station monitors the collaboration of other nodes and builds up a history that represents their reputation. Sensor nodes that contribute to common network operation increase their reputation. The reputation is used as a metric of trustworthiness and is used to statistically predict the future behavior of sensor nodes. The advantage of the proposed approach is that through the history created by the base station for each sensor node, and the negative reputation the base station assigns to any malicious behavior, it is possible to create routing paths consisting of less malicious nodes for more secure transmissions. Thus the malicious nodes are isolated. The main disadvantage of the proposed approach is when the number of malicious nodes in the sensor network increases, the success rate of the IDS decreases. This can be explained if we consider the fact that the IDS attempts to lower false positive and false negative rates and as a result the detection rate is decreased since it misses more malicious nodes. This technique may not be suitable for certain environmental monitoring applications, but may be considered in more critical applications in which an intrusion is likely and cannot be tolerated.

Doumit et. al. [18] propose a light-weight intrusion detection technique for wireless sensor nodes based on naturally occurring events and the analysis of fluctuations in sensor readings. Based on the Self-Organized Criticality (SOC) of the deployment region they acquire some knowledge, on which they deploy hidden Markov models (HMM). According to the proposed approach, the sensor network adapts to characterize the norm of the sensor network dynamics in its natural surroundings so that any unusual activities can be detected. Furthermore, the proposed approach is scalable to the addition of new sensor nodes. In order to avoid the transfer of a great amount of data to new sensor nodes and consequently consume scarce time and resources.

6.4. IDS for Specific Intrusions and Operations

Some other approaches propose intrusion detection techniques for specific intrusions and operations ([19], [20], [21], [22], [23]). Ngai et. al. [20] focus on Sinkhole attacks and propose a light-weight intrusion detection algorithm. The algorithm consists of two main steps. The first step is to create a list of the suspected malicious nodes by checking the data consistency. The identification of the intruder through the analysis of the network flow of information is performed during the second step. The algorithm focuses on the many-to-one communication mode and the solution explores the asymmetric property between the sensor nodes and the base station while effectively using the relatively high computation and communication power of the base station. They also consider the scenario in which a collection of cooperative malicious nodes attempt to hide the identity of the real intruder. They examine the suspicious nodes and attempt to identify the real attacker using majority voting.

Du et. al. [21] propose a general scheme for detecting localization anomalies caused by adversaries. They approach the problem as an anomaly intrusion detection problem, and they propose a number of ways to detect normalization anomalies. The proposed scheme exploits the topology deployment knowledge that is available in many network sensor applications and the group membership of each node's neighbors. It uses this knowledge in order to determine if the estimated location agrees with its observations. If there is an inconsistency above a certain threshold then it is assumed to be an indicator of malicious behavior. The inconsistency is formulated as an anomaly and the problem is studied as an anomaly detection problem. The simulation results demonstrate that the proposed framework is able to detect localization anomalies effectively even when a significant portion of a node's neighbors is compromised. Furthermore, the authors claim that the proposed scheme prevents the cause of an undetected large localization error since the more severe an attack is, the higher the detection time is and the lower the false positive rate is.

Wood et. al. [22] propose an approach for detecting and mapping jammed regions. They describe a mapping protocol whose goal is to surround a jammer. The jamming detection module monitors the radio and the medium access control layers. The protocol applies heuristics to determine if a node is jammed. After deciding that a node may possibly be jammed, is sends a message to its neighbors and notifies the application layer. The application layer may apply power management techniques in order to outlast the jamming. The mapping is initiated by the neighbors of the jammed node that have received jamming notifications. Each receiver of the notification message forms a group by adding nearby jammed nodes as jammed members. Even if the proposed approach is not able to prevent jamming, mapping the jammed area contributes substantially in the mitigation of its impact. Performance evaluation of the proposed approach demonstrates that regions can be mapped in 1-5 seconds when the network is at least moderately connected. Furthermore, the jamming detection and the mapping protocol may be viewed as a cheaper strategy since they use existing data and facilities in the typical sensor communication stack. We note that jamming attacks are often not lengthy in time and are launched at critical times to disable the network or conceal an adversary's activities, or misdirect an intrusion detection system. The authors assume partial jamming of the sensor network and that not all the jamming modules are themselves jammed.

Ye et. al. [23] propose a Statistical n-route filtering (SEF) of injected false data in sensor networks. In large-scale sensor networks individual sensors may be compromised. Compromised nodes might be exploited in order to inject erroneous sensing reports. If the compromised node is not detected then the erroneous reports may be forwarded to the base station causing not only false alarms, but also depletion of power resources. SEF can be used in order to detect and drop the erroneous reports.

7. Summary

Wireless sensor networks present a number of security challenges not faced by traditional wired or wireless networks. As a result, more research and practical experience is needed to develop effective wireless sensor network IDS. The design of an IDS for wireless sensor networks must take into consideration a number of factors. These factors include: the sensor communication protocol, the network topology, physical accessibility, application criticality, node redundancy, node mobility, computational resources, network membership requirements, base station network connectivity, and cryptographic support. This chapter maps the sensor network IDS landscape and provides a snapshot of the present state of research in this field. This chapter classifies wireless sensor network IDS in four distinct categories: IDS using routing protocols, IDS based on neighbor monitoring, IDS based on innovative techniques and IDS based on fault tolerance. A survey of research in this area reveals that most proposed solutions and results are theoretical or based on simulations, and that real-world experience in preventing, detecting, or responding to sensor network attacks has yet to be published. Since wireless sensor networks are most likely to be initially deployed as private networks, publicly available network traces, attack tools, and attack forensic information for researchers to study will be very limited. This makes it difficult to objectively evaluate and compare the performance of various sensor network IDS technologies. Publishing datasets of actual sensor network traffic and simulated or real intrusions would help researchers advance the state of the art and work from a common baseline in order to compare the effectiveness of their approaches.

References

[1] J. Hill, M. Horton, R. Kling and L. Krishnamurthy, The platforms enabling wireless sensor networks, *Communications of the ACM, Special Issue Wireless Sensor Networks* ,47, Issue 6, (June 2004), 41-46.

[2] T. Roosta, S. Shieh, and S. Sastry, A Taxonomy of Security Attacks in Sensor Networks and Countermeasures, *In Proceedings of the 1st IEEE International Conference on System Integration and Reliability Improvements*, Hanoi, Vietnam, 13-15 December 2006.

[3] I.Onat and A. Miri, An intrusion detection system for wireless sensor networks, In Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2005, 253–259.

[4] R. Roman, J. Zhou, J. Lopez, Applying Intrusion Detection Systems to Wireless Sensor Networks, *In Proceedings of 3rd IEEE Consumer Communications and Networking Conference, 2006*, (CCNC 2006), 1, 8-10 Jan 2006, Las Vegas, Nevada, USA, 640-644.

[5] I. Krontiris, T. Dimitriou, F. C. Freiling, Towards Intrusion Detection in Wireless Sensor Networks, t*o appear in Proceedings of the 13th European Wireless Conference*, 1-4 April 2007.

[6] A. P. R. da Silva, M.H.T. Martins, B. P.S. Rocha, A. A.F. Loureiro, L. B. Ruiz, 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, (2005)*, Montreal, Quebec, Canada, 16 – 23.

[7] F. Anjum, D. Subhadrabandhu, S. Sarkar and R. Shetty, On Optimal Placement of Intrusion Detection Modules in Sensor Networks, *In Proceedings of the 1st International Conference on Broadband Networks (BROADNETS'04)*, 25-29 October 2004, San Jose, California, USA, 690-699.

[8] T. Techateerawat, A. Jennings, Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks, *In Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06)*, Dec. 2006, Hong Kong, 227-230.

[9] A. Siraj, S. Bridges and R. Vaughn. "Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection System", IFSA World Congress and 20th NAFIPS International Conference 2001, 4, (2001), 2165-2170,.

[10] O. Kachirski and R. Guha, Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks, *In Proceeding of the IEEE Workshop on Knowledge Media Networking*, (2002), 153-158.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, *In Proceedings of the 6th ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'00)*, August 2000.

[12] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, Intrusion detection for sensor networks, *International Journal of Distributed Sensor Networks*, 2005.

[13] V. Bhuse, A. Gupta, Anomaly intrusion detection in wireless sensor networks Source, *Journal of High Speed Networks*, 15, Issue 1 (January 2006), 33 – 51.

[14] C.F. Hsin, M. Liu, A Distributed Monitoring Mechanism for Wireless Sensor Networks, *International Conference on Mobile Computing and Networking, In Proceedings of the 3rd ACM workshop on Wireless Security 2006*, Atlanta, GA, USA, 57 – 66.

[15] C.C. Su, K.M. Chang, Y.H. Kuo, The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks, *In Proceedings of IEEE Wireless Communications and Networking Conference 2005 (WCNC 2005)*, 13-17 March, 2005, New Orleans, LA USA, 4, 1927-1932.

[16] A. Agah, S. K. Das, K. Basu, and M. Asadi, Intrusion detection in sensor networks: A non-cooperative game approach, In Proceedings - Third IEEE International Symposium on Network Computing and Applications, NCA 2004, Aug 30-Sep 1 2004, 343–346.

[17] A. Agah, S. K. Das, Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach, *International Journal of Network Security*, Sept. 2007, 5, No. 2, 145-153.

[18] S. S. Doumit and D. P. Agrawal, Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks, in Proceedings of IEEE Military Communications Conference 2003 (MILCOM 2003), Oct 13-16 2003, 1 609–614

[19] O. Dousse, C. Tavoularis, P. Thiran, Delay of Intrusion Detection in Wireless Sensor Networks, *In Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, (MobiHoc'06), May 22–25, 2006, Florence, Italy, 155-165.

[20] E. C. H. Ngai, J. Liu, M.R. Lyu, On the Intruder Detection for Sinkole Attack in Wireless Sensor Networks, *In Proceedings of IEEE International Conference on Communications 2006 (ICC 2006)*, 8, June 2006, Instabul, Turkey, 3383-3389.

[21] W. Du, L. Fang and P. Ning, LAD: Localization Anomaly Detection for Wireless Sensor Networks, *In Proceedings of the 19th International Parallel and Distributed Processing Symposium (IPDPS'05)*, April 4-8, 2005, Denver, Colorado, USA.

[22] A. D. Wood, J. A. Standovic, and S. H. Son, JAM: A Jammed-Area Mapping Service for Sensor Networks, *In Proceedings of the 24th IEEE Real-Time Systems Symposium (RTSS)*, Dec 2003, 286-297.

[23] F. Ye, H. Luo, S. Lu, and L. Zhang, Statistical En-Route Filtering of Injected False Data in Sensor Networks, *In Proceedings of the 23rd IEEE INFOCOM*, Mar 2004, 2446-2457.