A Survey of Intrusion Detection Systems in Wireless Sensor Networks

Ismail Butun, Salvatore D. Morgera, and Ravi Sankar

***Abstract*—Wireless Sensor Networking is one of the most promising technologies that have applications ranging from health care to tactical military. Although Wireless Sensor Networks (WSNs) have appealing features (e.g., low installation cost, unattended network operation), due to the lack of a physical line of defense (i.e., there are no gateways or switches to monitor the information flow), the security of such networks is a big concern, especially for the applications where confidentiality has prime importance. Therefore, in order to operate WSNs in a secure way, any kind of intrusions should be detected before attackers can harm the network (i.e., sensor nodes) and/or information destination (i.e., data sink or base station). In this article, a survey of the state-of-the-art in Intrusion Detection Systems (IDSs) that are proposed for WSNs is presented. Firstly, detailed information about IDSs is provided. Secondly, a brief survey of IDSs proposed for Mobile Ad-Hoc Networks (MANETs) is presented and applicability of those systems to WSNs are discussed. Thirdly, IDSs proposed for WSNs are presented. This is followed by the analysis and comparison of each scheme along with their advantages and disadvantages. Finally, guidelines on IDSs that are potentially applicable to WSNs are provided. Our survey is concluded by highlighting open research issues in the field.**

***Index Terms*—intrusion detection, IDS, mobile ad hoc network, MANET, security, wireless sensor network, WSN.**

I. Introduction

OWING to their easy and cheap deployment features, Wireless Sensor Networks (WSNs[1]) are applied to various fields of science and technology: To gather information regarding human activities and behavior, such as health care, military surveillance and reconnaissance, highway traffic; to monitor physical and environmental phenomena, such as ocean and wildlife, earthquake, pollution, wild fire, water quality; to monitor industrial sites, such as building safety, manufacturing machinery performance, and so on [1].

On the other hand, security in WSNs is an important issue, especially if they have mission-critical tasks [2]. For instance, a confidential patient health record should not be released to third parties in a heath care application. Securing WSNs is critically important in tactical (military) applications where a security gap in the network would cause causalities of the friendly forces in a battlefield. Readers who are interested more on security in WSNs, may refer to [3], [4] and [5] for further information.

Security attacks against WSNs are categorized into two main branches: Active and Passive. In passive attacks, attackers are typically camouflaged (hidden) and either tap the communication link to collect data; or destroy the functioning elements of the network. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering/destruction and traffic analysis types. In active attacks, an adversary actually affects the operations in the attacked network. This effect may be the objective of the attack and can be detected. For example, the networking services may be degraded or terminated as a result of these attacks. Active attacks can be grouped into Denial-of-Service (DoS), jamming, hole attacks (blackhole, wormhole, sinkhole, etc.), flooding and Sybil types. Readers who are interested more on security attacks against WSNs, may refer to [4], [5] and [6] for further details.

Solutions to security attacks against networks (wireless and/or wired) involve three main components [7]:

- Prevention (defense against attack): This step aims to 'prevent' any attack before it happens. Any proposed technique will have to defend against the targeted attack.
- Detection (being aware of the attack that is present): If an attacker manages to pass the measures taken by the 'prevention' step, then it means that there is a failure to defend against the attack. At this time, the security solution would immediately switch into the 'detection' phase of the attack in progress and specifically identify the nodes that are being compromised.
- Mitigation (reacting to the attack): The final step aims to 'mitigate' any attack after it happens by removing (revoking from the network routing tables) the affected nodes and securing the network.

Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks). In a security system, if the first line of defense, "Intrusion Prevention," does not prevent intrusions, then the second line of defense, "Intrusion Detection," comes into play. It is the detection of any suspicious behavior in a network performed by the network members.

In any security plan, Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems: identification of the intruder, location of the intruder (e.g., single node or regional), time (e.g., date) of the intrusion, intrusion activity (e.g., active or passive), intrusion type (e.g., attacks such as worm hole, black hole, sink hole, selective forwarding, etc.), layer where the intrusion

Manuscript received September 22, 2012; revised February 6, 2013.

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA (e-mail: ibutun@mail.usf.edu, sdmorgera@usf.edu, sankar@usf.edu).

Digital Object Identifier 10.1109/SURV.2013.050113.00191

[1] See Appendix for the list of abbreviations used throughout this survey.

occurs (e.g., physical, data link, network). This information would be very helpful in mitigating (i.e., third line of defense) and remedying the result of attacks, since very specific information regarding the intruder is obtained. Therefore, intrusion detection systems are very important for network security.

WSNs have unique characteristics such as limited power supply, low transmission bandwidth, small memory size and data storage. Due to these restricted operating conditions (constrained computational and energy resources along with an ad hoc communication environment) of WSNs, most of the security techniques (including intrusion detection techniques) devised for traditional wired/wireless networks are not directly applicable to a WSN environment [8]. Designing an effective and efficient intrusion detection technique that is applicable to WSNs is a very big challenge, which motivated us to work on this research area. The first task of any research is to conduct an extensive literature review, which led us to the preparation of this survey as the first outcome of our research.

The rest of the paper is organized as follows: In Section II, a brief overview of IDSs, their classifications and their requirements is provided. Section III includes a brief survey of IDSs proposed for MANETs, followed by the comments regarding their applicability to WSNs. Section IV specifies the challenges and restrictions of WSNs and stresses the differences compared to the other types of networks (wired/wireless). Then, a detailed literature review on IDSs devised for WSNs is provided along with comments on their prominent and lacking features. Finally, our paper is concluded by comparing existing approaches, stressing their weaknesses and providing a general model for an IDS that would be applicable to WSNs.

II. Intrusion Detection Systems (IDSs)

In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intrusion Detection System (IDS) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions. Intrusion detection is typically one part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure [9]. In [10], intrusion is defined as: "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" and intrusion prevention techniques[2] (such as encryption, authentication, access control, secure routing, etc.) are presented as the first line of defense against intrusions. However, as in any kind of security system, intrusions cannot be totally prevented. The intrusion and compromise of a node leads to confidential information such as security keys being revealed to the intruders. This results in the failure of the preventive security mechanism. Therefore, IDSs are designed to reveal intrusions, before they can disclose the secured system resources. IDSs are always considered as a second wall of defense from the security point of view. IDSs are cyberspace equivalent of the burglar alarms that are being used in physical security systems today [12]. As mentioned in [10], the expected operational requirement of IDSs is given as: "low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected".

A. Requirements of IDSs

The IDS that is being designed should satisfy the following requirements:

- not introduce new weaknesses to the system,
- need little system resources and should not degrade overall system performance by introducing overheads,
- run continuously and remain transparent to the system and the users,
- use standards to be cooperative and open,
- be reliable and minimize false positives and false negatives in the detection phase.

B. Classification of IDSs

As shown in Fig. 1, IDSs can be classified as follows [13], [14], [15]:

1) Intruder type: Intruders to a network can be classified into two types:

- External intruder: An outsider using different means of attacks to reach the network.
- Internal intruder: A compromised node that used to be a member of the network. According to [16], insider attacks against ad-hoc networks use two types of nodes:
  - Selfish node: Uses the network resources but does not cooperate, saving battery life for their own communications. It does not directly damage other nodes.
  - Malicious node: Aims at damaging other nodes by causing network DoS by partitioning, while saving battery life is not a priority.

An IDS can detect both external and internal intruders, but it should be noted that internal intruders are harder to detect. This is due to the fact that internal intruders have the necessary keying materials to neutralize any precautions taken by the authentication mechanisms.

2) Intrusion type: Intrusions in a network may happen in various ways:

- Attempted break-in: An attempt to have an unauthorized access to the network.
- Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.
- Penetration: The acquisition of unauthorized access to the network.
- Leakage: An undesirable information flow from the network.
- DoS: Blockage of the network resources (i.e., communication bandwidth) to the other users.
- Malicious use: Deliberately harming the network resources.

IDSs may provide partial detection solution to those attacks. But of course, all system administrators would like to have a perfect IDS that would able to detect all of the intrusions listed above.

[2] For an application of intrusion prevention system to WSNs, please refer to [11].

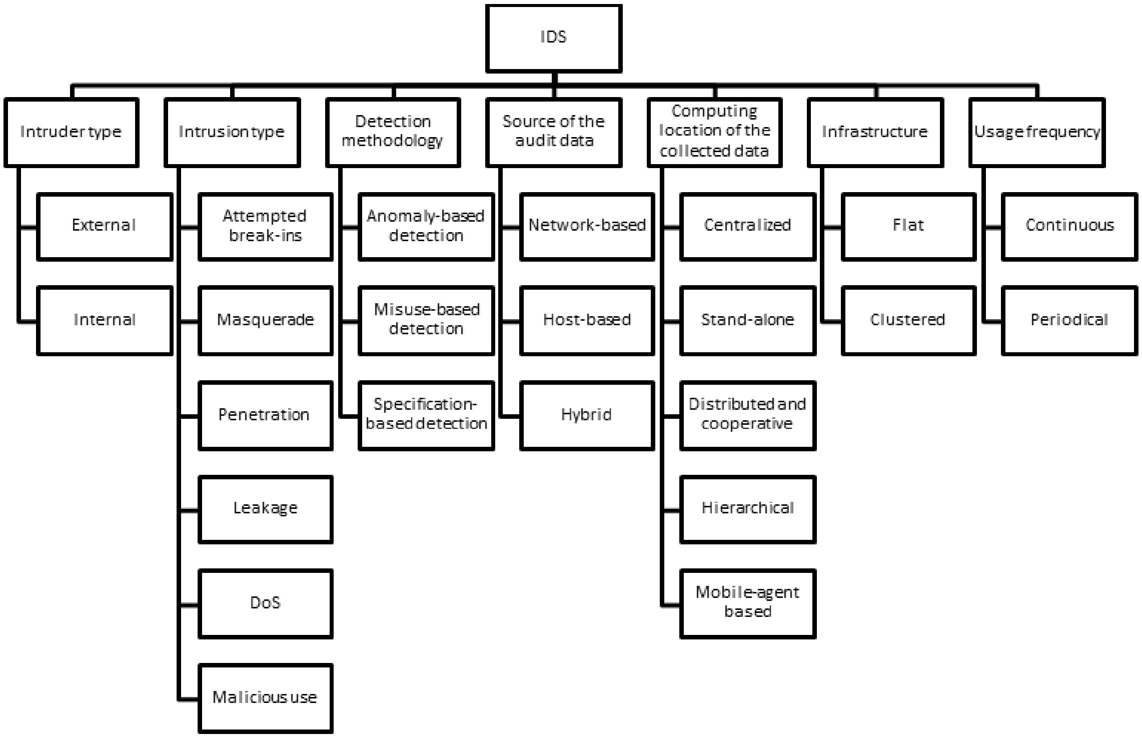


Fig. 1. Classification of IDSs.

3) Detection methodologies: IDSs are functionally categorized into three groups: anomaly based detection, misuse based detection, and specification based detection:

- **Anomaly based detection:** This is based on statistical behavior modeling. Normal operations of the members are profiled and a certain amount of deviation from the normal behavior is flagged as an anomaly. The disadvantage of this detection type is that the normal profiles must be updated periodically, since the network behavior may change rapidly. This may increase the load on the resource constrained sensor nodes. According to [17], this model detects intrusions in a very accurate and consistent way (low false positive and false negative rates) under the condition that the network being observed follows static behavioral patterns. The advantage of this detection type is that it is well suited to detect unknown or previously not encountered attacks. According to Garcia-Teodoro *et al.* [18], anomaly based IDSs are further divided into three categories according to the nature of the processing involved in the behavioral model considered. These categories are modified according to [12] and the final categorization is illustrated in Fig. 2:
  - Statistical based: In statistical based anomaly IDSs, the network traffic is captured and then a profile representing its stochastic behavior is generated. As the network operates in normal conditions (without any attack), a reference profile is created. After that, the network is monitored and profiles are generated periodically and an anomaly score is generated by comparing it to the reference profile. If the score passes a certain threshold, the IDS will flag an occurrence of the anomaly.
    - ∗ *Univariate:* Parameters are modeled as independent Gaussian random variables.
    - ∗ *Multivariate:* Correlations between two or more metrics are also considered here.
    - ∗ *Time series model:* Here, an interval timer is used along with an event counter that takes into account the order and inter-arrival times of the observations and also their values.

Statistical methods for anomaly detection are very well defined in [19] and here an example methodology for the detection of packet dropping attacks is summarized: Forwarding percentage (FP) of node *m*, is the ratio of forwarded packets by node *m* over the packets that are transmitted from node *M* to node *m* that are to be forwarded (in transit packets), observed for a specific period of time (τ). It is calculated as follows:

$$FP_m = \frac{packets\_actually\_forwarded}{packets\_to\_be\_forwarded} = \frac{\#(m,M) - \#([m],M)}{\#(M,m) - \#(M,[m])} \quad (1)$$

Where:

- ∗ m: monitored node
- ∗ M: monitoring node
- ∗ #(m,M): the number of outgoing packets from m of which node M is the next hop
- ∗ #([m],M): the number of outgoing packets from m of which node m is the source and node M is the next hop
- ∗ #(M,m): the number of outgoing packets from M of which node m is the next hop

- ∗ #(M, [m]): the number of outgoing packets from M of which node m is the final destination
- ∗ FP_m: forwarding percentage of node m

If the denominator of equation (1) is not zero and if $FP_m = 0$, then this event is detected as "Unconditional Packet Dropping" and m is identified as attacker. If the denominator of equation (1) is not zero and if FP_m is less than a certain threshold (T_{FP}) and following condition (2) holds then this event is detected as "Random Packet Dropping" and m is identified as attacker.

$$0 < FP_m < T_{FP} < 1 \qquad (2)$$

- – Knowledge based: Knowledge based anomaly IDSs rely on the availability of the prior knowledge (data) of the network parameters in normal operating condition as well as the one under certain attacks.
  - ∗ *Expert Systems:* It is based on rules classification of audit data.
  - ∗ *Description languages:* Diagrams (such as Unified Modeling Language (UML) diagrams) are generated based on the data specifications.
  - ∗ *Finite State Machine:* States and transitions are defined according to the available data set.
  - ∗ *Data clustering and outlier detection:* Observed data is grouped into clusters according to a specified similarity or distance measure. Points that do not belong to any cluster are named as the outliers.
- – Machine learning based: In machine learning based anomaly IDSs, an explicit or implicit model of the analyzed patterns is generated. These models are updated periodically, in order to improve the intrusion detection performance on the basis of the previous results.
  - ∗ *Bayesian networks:* It is based on probabilistic relationships among the variables of interest.
  - ∗ *Markov models:* It is based on stochastic Markov theory in which the topology and capabilities of the system are modeled as states that are interconnected through certain transition probabilities.
  - ∗ *Fuzzy logic:* It is based on approximation and uncertainty.
  - ∗ *Genetic algorithms:* It is inspired by the evolutionary theory of biology.
  - ∗ *Neural networks:* It is based on the human brain foundations.
  - ∗ *Principal Component Analysis (PCA):* It is based on a dimensionality reduction technique.

- **Misuse based (signature based or rule based) detection:** The signatures (profiles) of the previously known attacks are generated and are used as a reference to detect future attacks. For instance, a typical example of a signature would be: "there are 3 failed login attempts within 5 minutes" for the brute force password attack. The advantage of this type of detection is that it can accurately and efficiently detect known attacks; hence they have a low false positive rate. The disadvantage is that if the attack is a new kind (that was not profiled before), then the misuse detection would not be able to catch it. Sobh [13] pointed out that these systems are very much like the anti-virus systems, which can detect most or all known attack patterns, but are of little use for the attack methods that are unknown yet. On the other hand, in [20], the authors present the following rules in order to monitor the network anomalies:
  - – Interval rule: delay between the arrivals of two consecutive messages must be within certain limits.
  - – Retransmission rule: the transit messages should be forwarded by the intermediate nodes.
  - – Integrity rule: the original message from the sender must not deviate when it arrives to the receiver.
  - – Delay rule: the retransmission of a message must occur after a certain wait time.
  - – Repetition rule: same message can only be transmitted from the same node in certain number of counts.
  - – Radio transmission range: the messages should be originated from the neighboring nodes only.
  - – Jamming rule: the number of collisions for a packet transmission must be lower than a threshold.

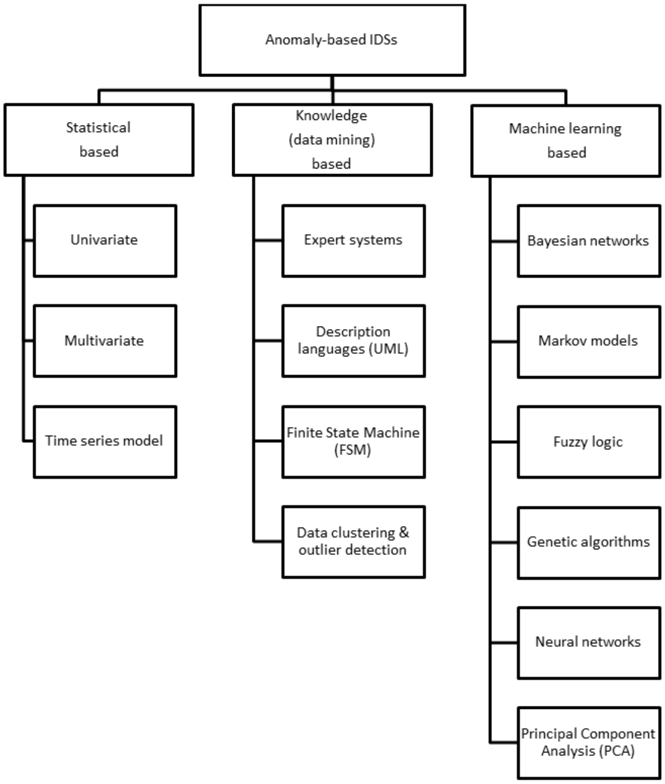


Fig. 2. Classification of anomaly based IDSs according to their detection algorithms

- **Specification based detection:** A set of specification and constraints that describe the correct operation of a program or protocol is defined. Then execution of the program with respect to the defined specifications and constraints is monitored [14]. This methodology was introduced in [21], which provided the capability to detect previously unknown attacks, while exhibiting a low false positive alarm rate.

Sobh [13] identified the main distinction among the anomaly based detection and misuse based detection as: “anomaly detection systems try to detect the effect of bad behavior but misuse detection systems try to recognize known bad behavior”.

Specification based intrusion detection techniques combine the advantages of both misuse and anomaly based detection techniques, by using manually developed specifications and constraints to characterize legitimate system behavior. Specification based intrusion detection techniques are similar to anomaly based detection techniques, in that both of them detect attacks as the deviations from a normal profile. Since specification based detection techniques are based on manually developed specifications and constraints, they have low false alarm rate compared to the high false alarm rated anomaly based detection techniques. On the other hand, the cost to achieve the mentioned low false alarm rate is that the development of detailed specifications and constraints would be very time consuming [22].

4) Source of the audit data: IDSs can be categorized into three groups, according to the source of the audit data (depending on the location of the data to be analyzed):

- Network based Intrusion Detection System (NIDS): NIDS passively or actively listens to the network transmissions, captures and examines packets that are being transmitted. NIDS can analyze an entire packet, payload within the packet, IP addresses or ports.
- Host based Intrusion Detection System (HIDS): HIDS is concerned with the events on the host that they are serving. They are capable of (but not limited to) detecting the following intrusions: changes to critical system files on the host, repeated failure access attempts to the host, unusual process memory allocations, unusual CPU activity or I/O activity. HIDS achieves this by either monitoring the real-time system usage of the host or by examining log files on the host.
- Hybrid Intrusion Detection System: It is composed of both NIDS and HIDS components in an efficient manner by the usage of the mobile agents. Mobile agents travel to each host and perform system log file checks while a central agent checks the overall network traffic for the existence of anomalies.

5) Computing location of the collected data: IDSs are divided into four categories according to the computing location of the collected data:

- Centralized IDS: A centralized computer monitors all the activities in the network and detects intrusions by analyzing the monitored network activity data.
- Stand-alone IDS: An IDS runs on each node independently and every decision is based on the information collected at its own node. Members of the network are not aware of the intrusions happening around them because stand-alone IDS do not allow individual nodes to cooperate or share information among each other. They work as if they are alone.
- Distributed and Cooperative IDS: This is proposed for flat network infrastructures. Each node runs an IDS agent which participates (cooperatively participating in the global intrusion detection decisions and actions) in the intrusion detection and response of the overall network. If a node detects an intrusion with weak or inconclusive evidence, then it can initiate a cooperative global intrusion detection procedure. If a node detects an intrusion locally with sufficient evidence, then it can independently alert the network regarding an attack.
- Hierarchical IDS: This is proposed for multi-layer (clustering) network infrastructures. Cluster heads (CHs) are responsible for monitoring their member nodes, as well as participating in the global intrusion detection decisions.
- Mobile Agent based IDS: Each mobile agent is assigned to perform a specific task of the IDS on a selected node; and the intrusion detection is performed by the cooperative action of these selected nodes. After a certain time period or after a specific task is done, agents may relocate to other pre-defined nodes in order to increase network lifetime and/or efficiency of the IDS. Specifications of mobile agents are provided as follows:
  - Mobility: Mobile agents bring the code to the data (to be processed) on a remote host for asynchronous execution. This would help to reduce the amount of the exchanged data significantly.
  - Autonomy: Mobile agents are given a mission upon their creation: they should be capable of achieving their tasks without any external help.
  - Adaptability: Mobile agents should adapt their behaviors according to the information they gather while performing their tasks.

6) Infrastructure: Anantvalee *et al.* [14] divided IDSs (for MANETs) into two groups according to their network infrastructures:

- Flat: All nodes are considered as equal in capabilities and they may participate in routing functions. This infrastructure is suitable for civilian applications, such as networking in a classroom or a conference.
- Clustered: All nodes are not considered as equal. Nodes within transmission range are grouped into a cluster and they elect a node as cluster head (CH) to centralize routing information for that cluster. Generally, CHs consist of more powerful devices with backup batteries, resulting in a longer transmission range. Therefore, CHs form a virtual backbone of the network. Depending on the routing protocol, intermediate gateways may relay packets in between the CHs. This kind of infrastructure model is very suitable for military applications having a command/control hierarchy.

7) Usage frequency: According to the usage frequency, IDSs are divided into two categories:

- Continuous (on the fly): The IDS monitors the network continuously.
- Periodical: The IDS monitors the network in certain periods of time.

C. Decision making in the IDS

There are two types of decision making mechanisms for IDSs:

- Collaborative decision making: All (or some) of the members of the network collaborate in making the decision regarding an event. For instance, in the case of majority voting, the final decision is made in favor of the majority of the members ending up with either of two decisions: "the event is an intrusion" or "the event is not an intrusion"
- Independent decision making: Each member concludes a decision regarding the events surrounding them.

According to [12], an IDS concludes either of four decisions (with non-zero probabilities) mentioned below as a result of the decision making process over an event:

- Intrusive but not anomalous (false-negative): There is an intrusion to the system, but the IDS fails to detect it and concludes the event as non-anomalous one.
- Not intrusive but anomalous (false-positive): There is no intrusion to the system, but the IDS mistakenly concludes a normal event as an anomalous one.
- Not intrusive and not anomalous (true-negative): There is no intrusion to the system, and the IDS concludes the event as non-anomalous one.
- Intrusive and anomalous (true-positive): There is an intrusion to the system, and the IDS concludes the event as an anomalous one.

For IDSs in WSNs, due to the nature of wireless communications, the following situations would result in false positives and hence, they need to be considered in the decision making model [16]:

- collisions
- packet drops
- limited transmission power
- fading battery power

D. Intrusion response

When an attack is possible to occur, the IDS does not take preventive measures, since the prevention part is left to the Intrusion Prevention System (IPS). The IDS works in a reactive way compared to the proactive way of the IPS. Whenever the intrusion alert is generated by the IDS, the following action(s) would be taken according to the system specifications:

- An audit record should be generated.
- All the network members, the system administrator (if he/she exists) and the base station (if it exists) should be alerted about the intrusion. If possible, location and identity of the intruder should be provided in the alert message.
- If it exists, a mitigation method should be induced in order to stop the intrusion. For example, an automated corrective action should be generated through a collaborative action of the network members (especially the neighboring members to the incident).

E. Related work and suggested readings

Readers, who are interested in the IDSs, can find more information (general information or specific areas other than WSNs) in the following papers:

- A very good classification of the IDSs is provided by Sobh [13].
- Classification of the IDSs for MANETs are provided by Ngadi *et al.* [9], Anantvalee and Wu [14], and Albers *et al.* [15].
- Garcia-Teodoro *et al.* [18], provided a survey of techniques, systems and challenges on the anomaly based NIDS.
- A brief survey of IDSs that are proposed for WSNs is provided in [23] and in contrast, our paper provides an extended survey with in-depth details comparing the proposed methods.
- A survey of IDSs for collaborative systems is provided in [24]. A more specific survey on alert correlation in collaborative intelligent IDSs is presented in [25]. Another work on decentralized multi-dimensional alert correlation for collaborative IDSs is provided in [26].
- A survey of IDS in cloud computing is provided in [27], which would be helpful to secure next generation networks.
- Garcia *et al.* [28] provides details of postmortem intrusion detection for cyber security systems and computer forensics. They show a classifier method for analyzing log files by using hidden Markov model.
- Evasion techniques that are threatening IDS are presented in Cheng *et al.*'s work [29]. They provide details of 5 different techniques (DoS, packet splitting, duplicate insertion, payload mutation, shell-code mutation) and assess the effectiveness of these techniques on 3 most recent IDSs.
- Please note that the IDS that are investigated in this survey are related to information and computer security; and they are not related to the topic of "Intrusion detection for perimeter protection". Readers who are interested in the later topic, please refer to the works presented in [30] and [31].
- Our survey does not include the methodologies and ideas that are proposed to secure the IDSs. Readers who are interested in that topic may refer to Shakshuki *et al.*'s [32] work.

III. IDSs PROPOSED FOR MANETs AND THEIR APPLICABILITY TO WSNs

The IDSs for MANETs are very well investigated and here a summary of the literature is provided, in order to help the reader with a better understanding of the current state of the art. Following each review, we will discuss about each of the proposed IDSs on their applicability to WSNs.

A. Agent based distributed and collaborative IDSs

The first article on intrusion detection for MANETs was written by Zhang and Lee [33]. They proposed an agent based distributed and collaborative IDS which is compliant with the Wireless Ad Hoc Network operating conditions.

As also mentioned in [14], the IDS agent described in [33] is composed of six blocks as shown in Fig. 3: The local data collection block is responsible for collecting real-time audit data (user activities, system call activities, communication

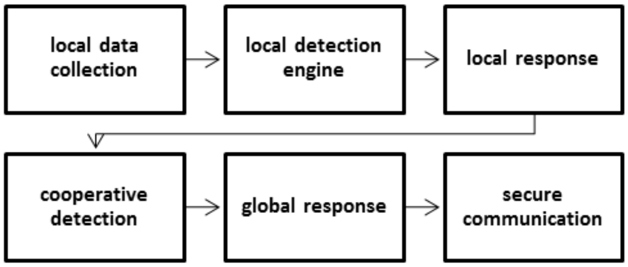


Fig. 3. Building blocks of an IDS agent

activities, and other traces) within its radio receiver range. This real-time audit data is analyzed by the local detection engine for the evidence of any kind of anomaly. In case of any anomaly detection, this block informs the local response and global response blocks (either one of them or both, depending the type of attack) in order to take a response against the anomaly (a possible intrusion). If the detection is inconclusive and needs more evidence, cooperation is conducted by the cooperative detection engine block and the communications with the neighboring agents needed for this cooperation is done through the secure communication block.

For each agent, there is a module to detect anomalies, called the "local detection engine". These modules have two components, namely:

- features: describes a logical event in the network such as the percentage of the route changes of a node's routing table.
- modeling algorithm: uses features as an input to the rule based pattern matching algorithm and then specifies whether the incidence is a normal or not according to the predefined matching criterion.

In their model, every node participates in the decision making process. After a certain threshold, the local IDSs trigger the global IDS which necessitate collaborative decision of the nodes neighboring the flagged node. This decision is made through a majority voting process. Detection is made by using the means of "entropy": The higher the entropy, the higher is the probability of anomaly. The proposed method is useful to detect only the attacks against the routing protocols; i.e., mis-routing, false route updating, packet dropping, DoS.

After anomalies are detected, depending on the level of the anomaly, either a local response is created or a global (collaborative) response is created among with the neighboring nodes. And communications pertaining to this global response should be assessed through secure communication links among the nodes. According to the authors, determining the features that would lead the modeling algorithm to detect anomalies with low percentage of false positive detection rates is a non-trivial task.

The authors used two types of classifiers: Decision tree and Support Vector Machine. Updates of the routing tables are chosen as a trace data in three ways: percentage of the changed routes, percentage of changes in the sum of hops of all the routes, and the percentage of newly added routes. Trace analysis and anomaly detection are the two main methods for the IDS that are used by the authors. Data obtained from normal network routing operation is fed to the training algorithm to obtain reference values of the classifiers. Then deviations (correlate) from normal profile classifiers are used to determine the anomalies in the network routing.

The devised method was tested on the ns-2 simulator for the following MANET routing protocols: DSR (Dynamic Source Routing; a reactive, source initiated, on-demand routing protocol), AODV (Ad-hoc On-demand Distance Vector; a reactive, source initiated, on-demand routing protocol), and DSDV (Destination Sequenced Distance Vector; a proactive, table-driven, routing protocol). According to the results, their algorithm performs better for on-demand protocols than proactive protocols, because it is easier to observe the correlation between the traffic patterns and routing message flows in on-demand protocols.

As an extension to their previous work, Zhang *et al.* [10] introduced the idea of multi-layer integrated intrusion detection and response, which is built upon the distributed and collaborative agent based IDS proposed in [33]. In the latest proposal, the intrusion detection module at each layer still needs to function properly, but detection on one layer can be initiated or aided by evidence from other layers. By this way, the authors claim that their IDS can achieve better performance in terms of both higher true positive and lower false positive detection rates. The proposed schemes might be applicable to WSNs in a sense that special care needs to be taken: As an example, they might be applied to a hierarchical WSN, where CHs might run the proposed schemes in a global sense and the sensor nodes in a local sense (division of labor).

Following the works of Zhang *et al.* ([10],[33]), Albers *et al.* [15] improved the distributed IDS structure by including mobile agents with the design. Mobile agents bring the code to the data, as opposed to traditional approaches where data is conveyed towards the computation location. By this way, asynchronous execution of the agent is performed on a remote host. This decreases the amount of data traffic (involving the agents) in the network significantly. On the other hand, it increases the individual work load of each node, which is not desirable in WSNs. Besides, transmission of mobile code (an executable portion of the IDS is transferred to the nodes for on-site data processing) would decrease the bandwidth of the WSN. So, this approach is not suitable if bandwidth efficiency is of prime importance.

Kachirski and Guha [34] further improved the mobile agent notion of [15] by providing efficient distribution of mobile agents with specific IDS tasks (network monitoring, host monitoring, decision making and action taking) according to their functionality across the wireless ad hoc network. This way, the workload of the proposed IDS is distributed among the nodes to minimize the power consumption and IDS related processing times by all nodes. Therefore, this scheme is applicable to WSNs. Another improvement is to restrict computation-intensive analysis of overall network security to a few nodes only.

B. Clustering (Hierarchical) based IDSs

In Kachirski and Guha's approach [17], regular nodes do not participate in the global decision making process. Only the

CHs are responsible for the global decision making process and the response. The main reason for this is to reduce the energy consumption. They wanted to conserve the energy of the majority of the nodes, by simply assigning them as subordinates under CHs.

In [19], clustering is used to select a single layer of sparsely positioned promiscuous monitors. These monitors are used to determine routing misbehavior via statistical anomaly detection. To conserve resources, a cluster based detection scheme is used in which a node is periodically elected as the intrusion detection monitoring agent within each cluster. In the proposed architecture, a detection agent runs on each monitoring node to detect local intrusions and then it collaborates with other agents to investigate the source of intrusion and coordinate responses.

In [35], the authors proposed a scheme that applies decentralized, cooperative intrusion detection approach for clustered MANETs. Dynamic hierarchy is used as an organizational model which allows higher-layer nodes to selectively aggregate and reduce intrusion detection data as it is reported upward from the leaf nodes to a root. This infrastructure not only allows intrusion detection observations to be gathered efficiently from the network, but also provides incremental aggregation, detection, and correlation as well as efficient dissemination of intrusion response and management directives. The proposed scheme is tested for the following three scenarios:

- Intentional data packet dropping
- Attacks on MANET routing protocol
- Attacks on network and higher-layer protocols

Clustering based IDSs would be beneficial for WSNs if they are applied with special care. Because, CHs would deplete their energies faster than the other nodes, which may cause segmentations (groups of nodes that are disconnected from each other) in the network. Therefore, extra batteries may have to be installed on CHs in order to help them to live longer, or CHs would be elected periodically in a sense that the node with the highest energy at each period would become the CH.

C. Statistical detection based IDSs

Puttini *et al.* [36] provides an intrusion detection algorithm based on Bayesian classification criteria. Their design is based on statistical modeling of reference behavior using mixture models in order to cope with an observable traffic composed of a mixture of different traffic profiles due to different network applications. It is focused on the detection of packet flooding, an example of a DoS attack, and scanning of attacks against MANETs. The proposed model builds a behavioral model that takes into account multiple user profiles and uses a posteriori Bayesian classification of data as a part of the detection algorithm.

In [37], the authors use estimated congestion at intermediate nodes to make decisions about malicious packet dropping behavior. They suggest that traffic transmission patterns should be used in concert with suboptimal MAC to preserve the statistical regularity from hop to hop. The proposed intrusion detection technique is a general one which is suitable for networks that are not bandwidth limited but have strict security requirements such as tactical networks. Therefore it is not applicable to WSNs that have limited bandwidth.

Statistical methods require too much data processing in order to sift the information that is valuable for statistics. Therefore, they are not applicable to WSNs.

D. Misuse detection based IDS

Nadkarni and Mishra [38] proposed an IDS based on a misuse detection algorithm. Their implementation focused on distance-vector routing protocols such as DSDV protocol. Their implementation aimed at detecting DoS and replay attacks as well as compromised nodes. Their simulation results have provided significant results about not only the accuracy and robustness of the scheme but also the non-degradability of network performance.

On the other hand, DSDV requires regular update for its routing tables which would not only deplete the energy resources of the nodes faster but also consume a portion of the valuable available bandwidth. Therefore, application of this algorithm to WSNs is not recommended.

E. Reputation (trust) based IDSs

A reputation based IDS scheme promotes node cooperation through collaborative monitoring of the nodes and a grading system associated with the results of the collaborative monitoring.

Michiardi and Molva [16] used the concept of reputation in order to evaluate a member's contribution to the network. The higher a member's reputation, the more selected connections can be made with other members of the network. This means that, members of the network would rather communicate with that particular node compared to the lower reputation ones, which would encourage members to increase their reputations. The authors defined three types of reputations:

- Subjective reputation: evaluated considering the direct interaction between a subject and its neighbors.
- Indirect reputation: evaluated by the non-neighbor members of the community.
- Functional reputation: subjective and indirect reputations calculated with respect to different functions (packet forwarding, route discovery, etc.).

Their collaborative reputation evaluation system consists of two basic components:

- Reputation Table: A data structure, stored on each node which includes the reputation data pertaining to a node.
- Watchdog Mechanism: Calculates pre-defined functional reputations according to the data stored at the reputation table and then detects misbehaving nodes. Detection is based on a threshold value (e.g., zero) of the reputation; if the reputation of a specific member drops below the threshold value, then the watchdog mechanism will deny any communications with that member.

DoS attacks were also of concern to them. Therefore, they proposed a generic mechanism based on reputation to enforce cooperation among the nodes. Besides, this reputation mechanism prevents DoS attacks resulting from selfish nodes.

CONFIDANT protocol [39] works as an extension to reactive source routing protocols, such as DSR, and uses a reputation based system that rates nodes based on their malicious behavior. Alarm messages coming from other nodes are evaluated and the reputation of the node under investigation is updated only if the messages are coming from the fully trusted nodes. A neighborhood watching scheme is used to detect intrusive activity made by the next node on the source route. When a node detects a malicious neighbor, it sends an alarm message to other nodes on its list of trusted neighbors. The overall protocol may be summarized in one sentence as: "Cooperation of nodes for the sake of fairness".

Both the proposed schemes ([16] and [39]) are applicable to WSNs with a slight modification: The renewal period of the reputation tables would be decreased, in order to increase the bandwidth efficiency.

F. Zone based IDS

With Zone based IDS of Sun *et al.* [40], the network is divided into non-overlapping zones and each IDS agent broadcasts locally generated alerts inside the zone. Gateway zones are responsible for aggregation and correlation of locally generated alerts. Only gateway nodes can generate network wide alarms. Alerts indicate possible attacks and are generated by local IDS agents, while alarms indicate the final detection and can be generated only by gateway nodes.

The functionality of their proposed *local aggregation and correlation engine* is to locally aggregate and correlate the detection results of detection engines. Whereas, the functionality of their proposed *global aggregation and correlation engine* in gateway nodes is to aggregate and correlate the detection results from local nodes in order to make final decisions.

Local alerts are generated according to two detection criteria: 1) Percentage of change in route entries, which represents the deleted and newly added routing entries in a certain time period; 2) Percentage of change in number of hops, which represents the change of the sum of hops of all routing entries in a certain time period.

According to the authors' simulations (performed on GloMoSim network simulator), their model responded with fewer false positives as the mobility decreased. Besides, aggregation algorithm of gateway nodes achieved much lower false positives than the IDS of local nodes, because they can collect information from a wider area and make more accurate decisions.

The proposed model detects intrusions in the routing layer of the OSI stack but it ignores other layers. Since the attacks happening in other layers would not be detected by this model, it is a partial IDS.

The proposed scheme requires each node to have the geographical information surrounding them. Although this is possible by integrating global positioning system (GPS) receiver to the nodes in MANETs, it is not feasible in WSNs, because most sensor nodes are not generally equipped with GPS due to the cost and energy restrictions.

G. Game theory based IDSs

In [41] and [42], the authors present a game-theoretic method to analyze intrusion detection in MANETs. They use game theory to model the interactions between the nodes of an ad hoc network. They model the interaction between an attacker and an individual node as a two player non-cooperative game. According to their assumptions, as long as the beliefs are consistent with the information obtained and the actions are optimal given the beliefs, the model is theoretically consistent.

The proposed schemes need a central processing unit in order to process all the observations collected by the monitoring mechanism. This requires a high speed microprocessor as well as a large memory space to store the data to be processed. Therefore, in order to apply these schemes to WSNs, one should pick a centralized WSN, where a base station (BS) equipped with a computer that has high speed processing power and large memory. Besides, the schemes should be modified to decrease the traffic load in between each node and the BS. For example, a logging mechanism can be used, where each node may store information regarding the data interactions with other nodes (and also if possible with the attackers). Then, these logs may be sent to the BS for the application of the game theory based detection.

H. Genetic algorithm based IDS

Sen and Clark [43] investigated the use of evolutionary computation techniques to discover detectors suited to complex (lack of central computing unit, highly mobile nodes, limited resources) MANET environment. Authors applied grammatical evolution and genetic programming techniques to detect ad hoc flooding and route disruption attacks on AODV. Authors showed that their evolved programs performed good on simulated networks with varying mobility and traffic patterns.

Although this methodology might be very promising for MANETs where most of the nodes (e.g., PDAs) are powerful enough to run such energy consuming algorithms, it is not applicable to WSNs where sensor nodes have limited capacity for data processing and storage.

I. Other works

In [44], the watchdog mechanism is implemented on top of DSR protocol to verify that when a node forwards a packet, the next node in the path also forwards the packet; otherwise the next node is announced as misbehaving. Watchdogs run on each node, listens to transmissions of the neighboring nodes in a promiscuous mode. Watchdogs may not always be effective because of the packet collisions. The proposed watchdog mechanism is applicable to WSNs.

Wai *et al.* [45] proposed a hybrid IDS that can both work on wired networks as well as wireless ad hoc networks. The proposed model promises to use both anomaly and misuse detection algorithms. Both the details of the proposed model and the implementation results were not provided, thus making it impossible to compare its performance to the previously proposed models. Besides, the proposed scheme requires an end-to-end secure communication channel between nodes, which generally does not exist in WSNs.

MANETs became very useful for tactical networks such as command posts, vehicle convoys, autonomous robot systems, and also for infantry troops. The authors of MITE (MANET Intrusion Detection for Tactical Environments [46]) aim at developing prototypical solutions for intrusion detection in MANETs, especially in tactical scenarios. The results of MITE have been realized and evaluated as real-world implementations besides the simulation results. The authors proposed a robust and resource saving sensor detector infrastructure as well as supporting components. The TOGBAD module of the proposed scheme uses a significant amount of the network traffic. Therefore, it is not applicable to WSNs, where the bandwidth is a scarce resource and needs to be utilized very efficiently.

Wei and Kim [47] used traffic prediction to detect intrusions in wireless industrial networks. Authors proposed a data traffic prediction model based on autoregressive moving average (ARMA) using the time series data. According to their simulations, the model quickly and precisely predicted the network traffic and sifted out the attackers. Although the achievements seems promising, the proposed method brings extensive traffic load to the network for the sake of the monitoring data packets and also requires a centralized processing unit to store and analyze the whole traffic data, which are not provided in WSNs.

Readers who are interested in IDSs designed for MANETs would find more information in the following papers:

- Brutch and Ko [21] provided a brief overview of research efforts on IDS for wired networks and wireless ad hoc networks. Besides, they provide classifications and different architectures of IDSs and stress on their limitations in wireless ad hoc operation environment. They mention the methods to detect the attacks against the routing infrastructure and also methods to detect the attacks against mobile nodes.
- Mishra *et al.* [48] provided a brief introduction of MANETs and IDSs, and then summarized the key features of the IDSs proposed in the literature. They provided a survey on IDSs devised for MANETs.
- Sun *et al.* [22] provided a brief overview of intrusion detection techniques and a thorough survey on IDSs in MANETs. They also provided a literature overview of intrusion prevention algorithms proposed for WSNs. The article is written from the point view of secure in-network data aggregation.
- Sen and Clark [49], provided a survey of IDSs for MANETs. According to the authors, intrusion detection for MANETs is a complex and difficult task due to the dynamic nature of MANETs, their highly constrained nodes and the lack of central monitoring points.
- Ngadi *et al.* [9] also provided a brief survey of IDSs for MANETs.

J. Summary and future remarks

In this section, we presented IDSs that have been proposed for MANETs and discuss their applicability to WSNs. Some systems would be applicable directly (generic proposals), some would be applicable with major modifications, while the rest would not be applicable to WSNs (specific proposals), simply because of the unique design requirements of WSNs. Table I summarizes the schemes discussed so far, in terms of their detection technique and their applicability to WSNs.

Clustering (hierarchical networking) would be beneficial in adapting MANET IDS schemes to WSNs. For instance, consider the application of agent based IDS of [10] to a clustered WSN. The proposed IDS scheme would be divided into two categories as follows: Global IDS agents would be installed (with a full version of the scheme) on CHs; whereas local IDS agents would be installed (with a light version of the scheme excluding the global components) on each sensor node as shown in Fig. 4. After two or more local IDS agents report the occurrence of an event, a global IDS agent would take charge and run a global detection sequence throughout the network. By running the full version of the scheme only on CHs and running the lighter version on the sensor nodes, the energy consumption of the whole scheme on the WSN would be significantly decreased and as a result, total life time of the network would be increased.

IV. IDSs PROPOSED FOR WSNs

Intrusion detection in WSNs is becoming a key research topic addressed in the literature. Therefore, in this section, the research done so far in this field is summarized. Before starting, in section IV-A, the unique challenges of WSNs that make it difficult to apply traditional (designed for wired or generic wireless networks) IDSs are presented. WSNs are special version of MANETs, with very specific design restrictions. Therefore, in section IV-B, the key differences of both networks will be mentioned. Finally, in section IV-C, the state-of-the-art IDSs in the literature of WSNs will be provided. Following all the reviews, we will discuss about advantages and disadvantages of each scheme and provide a comparison chart.

A. Constraints and Research Challenges in WSNs

The proliferation of WSNs led researchers to develop strategies about providing stable communications and networking for distributed network environments, and also about how to secure these strategies with limited resources. The lack of fixed infrastructure (i.e., gateways, routers, base stations, etc.) makes the design of security related models and algorithms for WSNs more difficult. Bandwidth, throughput, battery power are the scarce resources that need to be used with great consideration. Following is a brief list of constraints and the corresponding challenges they bring to WSNs:

- There is no infrastructure in WSNs to support operations such as communications, routing, real time traffic analysis, encryption, etc.
- Nodes are prone to physical capture, tampering or hijacking which compromises network operations.
- Compromised nodes may provide misleading routing information to the rest of the WSN leaving the network un-operational (blackhole, wormhole, sinkhole attacks).
- Wireless communication is susceptible to eavesdropping, which would reveal important data to adversaries and/or to jamming/interfering, which would cause DoS in the WSN.
- There is no trusted authority; decisions have to be concluded in a collaborative manner.

In designing an IDS for WSNs, these constraints and challenges should be considered.

TABLE I
PROPOSED IDSS FOR MANETS AND THEIR APPLICABILITY TO WSNS.

Proposed system	Detection technique	Applicability to WSNs
Zhang and Lee [10] [33]	distributed and collaborative	applicable with modification
Albers *et al.* [15]	distributed and collaborative	not applicable
Michiardi and Molva [16]	reputation	applicable with modification
Kachirski and Guha [17]	clustering	applicable with modification
Kachirski and Guha [34]	distributed and collaborative	applicable
Huang and Lee [19]	clustering	applicable with modification
Sterne *et al.* [35]	clustering	applicable with modification
Puttini *et al.* [36]	statistical	not applicable
Rao and Kesidis [37]	statistical	not applicable
Nadkarni and Mishra [38]	misuse	not applicable
CONFIDANT protocol [39]	reputation	applicable with modification
Sun *et al.* [40]	zone based	not applicable
Patcha and Park [41] [42]	game theory	applicable with modification
Marti *et al.* [44]	watchdog	applicable
Wai *et al.* [45]	hybrid	not applicable
MITE protocol [46]	network monitoring	not applicable
Sen and Clark [43]	genetic algorithms	not applicable
Wei and Kim's [47]	autoregressive moving average	not applicable

B. Differences between MANETs and WSNs

Roman *et al.* [50], stressed the fact that the IDSs that are designed for MANETs cannot be applied to WSNs directly. Since MANETs are mobile and IDSs for them are designed in the same manner, they will be less effective in a stationary network such as WSNs. Following are basic distinctive features that differentiate WSNs from MANETs:

- Mobility: Compared to mobile MANET nodes, WSN nodes are generally stationary.
- Computational capacity: WSN nodes have limited computational power compared to the MANET nodes. A typical sensor node such as MICAz [51] runs an Atmel ATmega128L processor with a maximum speed of 16 MHz [52], whereas a typical MANET node, such as generic commercial laptop, may have a processor with a maximum speed of 4 GHz [53].
- Communications range: The range of communication is around 20-30 meters for WSN nodes (for MICAz [51]), whereas it is up to 100 meters for MANET nodes (for XBee WiFi module [54]).
- Communications bandwidth: The communication bandwidth is limited to 250 kbps (for a typical MICAz mote [51]) data rate in WSNs, whereas it goes up to 65 Mbps (for a typical XBee WiFi module [54]) data rate in MANETs.
- Power supply: WSN nodes have a very limited power supply, such as 2 AA sized batteries for MICAz motes [51] (with an approximate energy capacity of 10 Wh), whereas MANET nodes generally have a bigger battery, such as laptop batteries (with an approximate energy capacity of 150 Wh). Obviously, this would affect their lifetime directly. Assuming that their power consumption rates are the same, MANETs would have approximately 15 times more life time compared to WSNs.
- Autonomy: In MANETs, every node is managed by a human user, whereas in WSNs every node is autonomous in a sense that it receives and sends data from/to the base station (BS). BS is generally managed by a human but not the sensor nodes.
- Node density: Node density in WSNs is higher than that in MANETs. On the other hand, WSNs nodes are more susceptible to hardware failures (battery constraints, lacking physical security, etc.), which would decrease the node density with advancing time.

These distinctive features should be considered before adapting an IDS that is designed for a MANET to a WSN.

C. Proposed Schemes

1) Clustering (Hierarchical) based IDSs: In [55], a hierarchical framework for intrusion detection as well as data processing is proposed. Throughout the experiments on the proposed framework, they stressed the significance of one-hop clustering. The authors believed that their hierarchical framework was useful for securing industrial applications of WSNs with regard to two lines of defense.

In [56], the authors proposed an isolation table to detect intrusions in hierarchical WSNs in an energy efficient way. Their proposal required two-levels of clustering. According to their experiment, their isolation table intrusion detection method could detect attacks effectively. The problem with this proposal is as follows: The authors claim that each level monitors the other level and report any anomalies to the base station. Since it is a hierarchical network, any alert generated by the lower level nodes must pass through the higher level nodes. In the case that the higher level node is the intruder, it will not allow the BS to be aware of its misbehavior by simply blocking the alert messages it receives from the lower level nodes.

In [57], an IDS based on clustering approach was proposed. Their proposal also ensured the security of the CHs. In their approach, members of a cluster monitor their CH in a time scheduled manner. In this way, energy for all cluster members is saved. On the contrary, cluster members are monitored by the CH, not by the contribution of cluster members. This also saves the energies of the cluster members. Through simulations, the authors showed that their proposed algorithm is much more efficient compared to other algorithms in the literature. The problem with this approach is its key

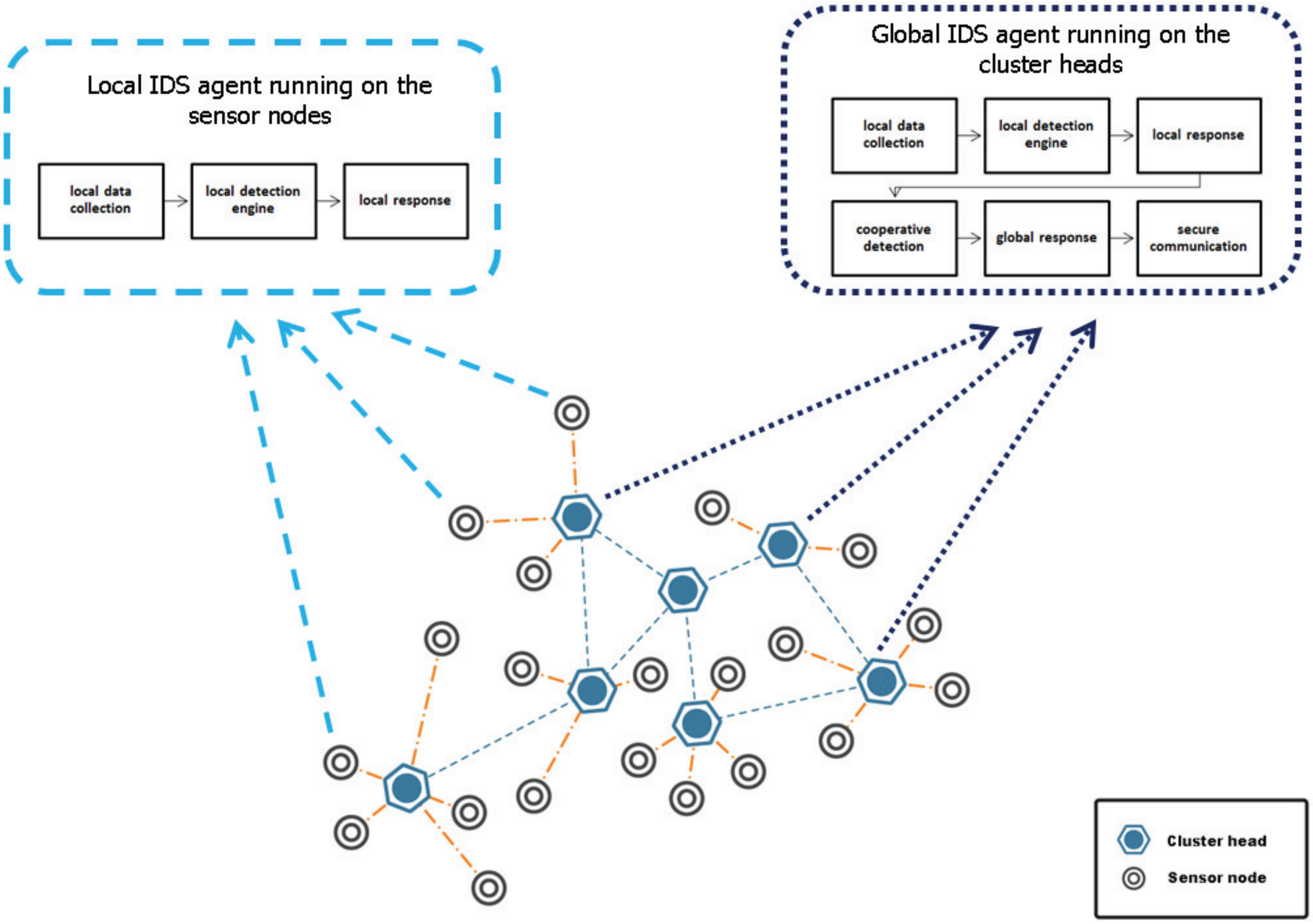


Fig. 4. Application of an IDS devised for a MANET to a WSN by using clustering approach.

management mechanism. It is a part of the IDS and helps IDS to establish pairwise keys among the nodes. The IDS uses these keys through the authentication of the messages. The key management assumes that the nodes are stationary (non-mobile) and the new nodes cannot be added after the pairwise keys are established. This constitutes a handicap for the model considering the fact that WSN may periodically require deployment of new nodes.

In [58], the authors incorporated a hierarchical IDS model in which the network is divided into clusters and for each cluster, a CH is elected. They issued centralized routing, meaning that every packet of transmitted data will be forwarded to the CH and then to the base station. Their proposal included a method to place intrusion detectors in the CHs so that the entire network is covered with a minimum number of detectors. The authors did not provide any simulation results or any real experimental data. So, it is not clear whether the system would perform as promised.

In [59], a distributed cluster based anomaly detection algorithm was proposed. They minimized the communication overhead by clustering the sensor measurements and merging clusters before sending a description of the clusters to the other nodes. The authors implemented their proposed model in a real-world project. They demonstrated that their scheme achieves comparable accuracy when compared to centralized schemes with a significant reduction in communication overhead.

2) Distributed and collaborative IDSs: Krontiris *et al.* [60] proposed a distributed IDS for WSNs based on collaborative neighborhood watching. In a simulation environment, the authors evaluated the effectiveness of their IDS scheme against blackhole and selective forwarding attacks.

In [61], a solution to the problem of cooperative intrusion detection in WSNs was proposed, where the nodes were equipped with local detector modules and have to identify the intruder in a distributed way. The detector modules triggered suspicions about an intrusion in the sensor's neighborhood. The authors presented necessary and sufficient conditions for successfully exposing the attacker and a corresponding algorithm that is shown to work under a general threat model.

In [20], the proposed IDS used a specification based detection algorithm. The authors used a decentralized approach of detection in which intrusion detectors were distributed among the network (their distance was one-hop, covering the entire network). The collected information and its processing were performed in a distributed fashion. They claimed that this distributed approach was more scalable and robust compared to a centralized approached owing to the fact that the intrusion detectors had different views of the network by being distributed to all over the network.

3) Statistical detection based IDSs: Ngai *et al.* [62] presented an algorithm to detect the intruder in a sinkhole attack. The proposed algorithm first finds a list of suspected nodes and then effectively identifies the intruder in the list through a network flow graph. The algorithm implements a multivariate technique (statistical - parametric technique) based on the chi-square test. Effectiveness and accuracy of the proposed algorithm is verified by both numerical analysis and simulations. The authors claimed that their algorithm's communication and computational overheads are reasonable for WSNs.

In the proposed algorithm of [63], the sensor network adapts to the norm of the dynamics in its natural surroundings so that any unusual activities can be singled out. In order to achieve this, they employ a hidden Markov model. The authors claimed that their proposed algorithm is easy to employ, requiring minimal processing and data storage. The functionality and practicality of the algorithm is shown through experimental scenarios. The proposed algorithm sifts out any unusual readings by using the statistical approach. So it is a very specific kind of IDS that is mainly focused on the accuracy of the data gathered rather than the security of the nodes or the links.

In [64], the authors proposed a real time, node based anomaly detection algorithm that observes the arrival processes experienced by a sensor node. They developed an arrival model for the traffic that can be received by a sensor node and devised a scheme to detect anomalous changes in that arrival process. The detection algorithm kept short term statistics using a multi-level sliding window event storage scheme. In this way the algorithm could compare arrival processes at different time scales. The authors claimed that their algorithm was resource aware and has low complexity.

4) Game theory based IDSs: In [65] and [66], Agah *et al.* considered attack and detection as both participants of the game and formulated strategies for both parties. In order to increase detection probability, strategies were normalized into a non-cooperative, non-zero game model. Both schemes focused on determining the weakest node in the network and then providing strategies to defend that node. The problem with this approach was that there might be multiple intrusions to the WSN and only one of them would be caught by the IDS while leaving others undetected.

5) Anomaly detection based IDSs: In [67], Rajasegarar *et al.* provided a survey article about the state of the art in anomaly detection techniques for WSNs. They suggested for the researchers (for anomaly detection) to consider the inherent limitations of WSNs in their design so that the energy consumption in sensor nodes is minimized and the lifetime of the network is maximized.

In [68], the same authors proposed a solution to the problem of minimizing the communication overhead in the network while performing in-network computation when detecting anomalies. Their approach to this problem is based on a formulation that uses distributed one-class quarter-sphere support vector machines to identify anomalous measurements in the data. Data vectors are mapped from the input space to a higher-dimensional space for further investigations. The authors implemented their proposal in a real-world project and they claimed that their model was energy efficient in terms of communication overhead while achieving comparable accuracy to a centralized scheme.

Bhuse and Gupta [69] proposed lightweight methods to detect anomaly intrusions in WSNs. Their main idea was to reuse the already available system information (such as neighbor lists, routing tables, sleep/wake-up schedules, receive signal strength indication, MAC layer transmission schedules) that was generated at various OSI layers of a network protocol stack, especially the physical, MAC and routing layers. In order to have a better detection rate, the authors proposed multiple detectors monitoring different layers of the OSI stack. This is not feasible for WSNs, because intrusion monitoring in different layers and sustaining the coordination of these monitors may rapidly deplete the scarce resources of the WSN. Besides, the authors proposed their schemes for outsider attacks only, ruling out the insider attacks. This is inadequate choice, because sensor nodes in a WSN are very vulnerable to insider attacks such as physical capture attack, Sybil attack, etc.

Onat and Miri [70] provided an IDS for WSNs that was based on detection of packet level receive power anomalies. The detection scheme was focused on transceiver behaviors and packet arrival rates of the neighboring nodes of a particular node. WSNs are rarely mobile and therefore they have a stable communication pattern when compared to MANETs. The authors exploited this specific distinction. Each node built a simple statistical model of its neighbors' behavior and used this statistics to detect any abnormal changes in the future. The proposed model worked well to detect impersonation attacks.

6) Watchdog based IDS: Roman *et al.* [50] provided guidelines about application of IDSs (that are designed for MANETs) to static WSNs. Then, they propose an IDS for WSNs called 'spontaneous watchdogs' in which the neighbors are optimally monitored and where some nodes choose to independently monitor the communications in their neighborhood.

7) Reputation (Trust) based IDS: Wang *et al.* [71] proposed an IDS for WSNs that uses packet marking and then heuristic ranking algorithms to identify most likely bad nodes in the network. Each packet is encrypted and padded so as to hide the source of the packet. The packet mark is added in each packet such that the data sink can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. According to their simulations, most of the bad nodes could be identified by their *heuristic ranking algorithm* with small false positive rate.

Bao *et al.* [72] proposed a hierarchical trust management for WSNs to detect selfish and malicious nodes. Authors developed a probability model utilizing *stochastic Petri nets technique* to analyze the protocol performance and validated subjective trust against objective trust obtained based on ground truth node status. Their trust-based IDS algorithm outperforms anomaly-based IDS algorithms in the detection probability percentage while maintaining sufficiently low false positive rates.

TABLE II
COMPARISON OF THE IDSS PROPOSED FOR WSNS

Proposed system	**Architecture**	**Detection technique**	**Highlighting features**
Da Silva *et al.* [20]	Distributed	Rule based approach (interval rule)	Scalable, robust and fast intrusion detection.
Roman *et al.* [50]	Distributed and Cooperative	Spontaneous watchdogs	Relies on the broadcast nature of sensor communications and takes advantage of the high density of sensors being deployed in the field.
Chen *et al.* [56]	Hierarchical	Rule based approach	Uses monitoring group of nodes and routing tables for detection
Su *et al.* [57]	Hierarchical	Rule based approach (packet dropping rate)	Saves energy, extends the network lifetime. On the other hand, new nodes cannot be added to the network.
Strikos [58]	Hierarchical	Rule based approach	Combined already existing approaches, in order to achieve a more complete solution. Neither simulation results, nor real world experimental results are provided.
Rajasegarar *et al.* [59]	Hierarchical	Specification based approach, data clustering (standard deviation from the average inter-cluster distance)	Achieved comparable performance with the centralized schemes.
Krontiris *et al.* [60]	Distributed and Cooperative	Rule based approach (packet dropping rate)	Detects only blackhole and selective forwarding attacks. Besides, proposed solution works only when there is one attacker.
Krontiris *et al.* [61]	Distributed and Cooperative	Specification based approach	Proposed solution works only when there is one attacker.
Ngai *et al.* [62]	Centralized (BS)	Statistical based anomaly detection (parametric), routing pattern anomalies	Specified to detect Sinkhole attacks only.
Doumit and Agrawal [63]	Hierarchical	Statistical anomaly based approach (parametric), hidden Markov model	Focused on the accuracy of the data gathered, rather than the security of the nodes or the links.
Onat and Miri [64]	Stand alone	Statistical based anomaly detection (real time traffic on the nodes, arrival process)	Keeps short term dynamic statistics using a multi-level sliding window event storage scheme. The scheme works on each node, therefore the detections are local and nodes are not aware of the attacks globally (network-wide).
Agah *et al.* [65] [66]	Hierarchical	Game theory along with Markov decision process	Only one of the clusters of the network is monitored at a time. This leaves the rest of the network un-protected.
Bhuse and Gupta [69]	Stand-alone	Rule based approaches (for physical, MAC, routing and application layers)	Proposed lightweight techniques that would detect anomalies at all layers of a network stack in WSNs.
Onat and Miri [70]	Distributed and Cooperative	Statistical anomaly based approach (average receive power and average packet arrival rate)	Exploits the stability of the neighborhood information of the WSN nodes.
Rajasegarar *et al.* [68]	Distributed	Anomaly based approach, support vector machine	Minimizes communication overhead while performing in-network anomaly detection.
Wang *et al.* [71]	Centralized (data sink)	Reputation based approach	Uses heuristic ranking algorithms to identify most likely bad nodes in the network.
Bao *et al.* [72]	Hierarchical	Reputation based approach	Uses high scalable cluster-based hierarchical trust management protocol to effectively identifying the selfish and malicious nodes.

D. Issues concerning the proposed schemes

IDSs proposed for WSNs are summarized in Table II including their required network architecture, detection technique and highlighting features of each scheme. Accordingly, the following conclusions can be drawn for the proposed IDSs in WSNs:

- In hierarchical, clustering based IDSs, clustering algorithms may consume considerable amount of the network's energy through the formation of the clusters. After the clusters are formed and the CHs are elected, CHs may constitute a single point of failure and they have to be secured. Besides, if the CH is not a special node (more powerful), then the overhead of being a CH will diminish its resources very quickly.
- Agent based IDSs reduce the network load and latency. On the other hand, they cause high energy consumption of the nodes they are working on. Communication cost between agents and coordinator, or in between agents, may cause congestion and bottle neck in the network.
- Rule based IDSs are simple to install and easy to operate. On the other hand, they need continuous rule updates in order to cope with the new released attacks.
- Data mining based IDSs can detect unknown attacks. Unfortunately they have high computational complexity and high energy consumption requiring large amounts of data samples. Besides, they also need efficient analytic tools to analyze large amount of audit data and a mass memory space to store them.
- In game theory based IDSs, the detection rate can be adjusted by the network security administrator through changing the parameters. The problem with this system is that it is non-adaptive and requires human intervention for a stable operation.

V. FUTURE DIRECTIONS IN THE SELECTION OF IDS FOR WSNS

Energy consumption of the IDSs is an important issue from a system design point of view. WSNs consume energy through sensing the surrounding phenomena, processing the sensed information and transmitting the resultant data. Therefore, the IDSs need to spend the least amount of energy as possible to spare enough energy for the crucial operations of the WSN. As a result of this low energy consumption requirement of WSNs, it is beneficial to use a hierarchical model for IDSs. This means that the network would be divided into clusters, each of which will have a CH. Accordingly, the energy consumption will be minimized by avoiding the need for all the nodes to send data to the BS. Besides, high energy consuming IDS algorithms would run only on the CHs which would save energy on the rest of the nodes and ultimately increase the total lifetime of the network.

Since there are a variety of intrusion detection algorithms available, the selection of the intrusion detection technique would be specific to the requirements of the intended application; i.e., the attacks that need to be detected, the accuracy of the detection (percentage of the false positives and true positives), and the duration of the detection time.

Our suggestion for the selection of the IDS for WSNs will be application specific (various suggestions for different applications):

- For the mobile applications, where sensor nodes are in movement, we recommend the usage of distributed and cooperative IDS schemes, as they are scalable, robust and fast. Da Silva *et al.*'s [20], Roman *et al.*'s [50] and finally Onat and Miri's [70] proposed schemes are recommended as the most promising ones among those presented in Table II.
- For the stationary applications, where there is a centralized computing unit at BS or at data sink, we recommend the usage of centralized IDS schemes, as they are powerful and can detect whole range of attacks. Among the schemes presented in Table II, Wang *et al.*'s [71] proposed scheme is recommended for adopting or can be a good starting point to build on it.
- For the cluster based applications, where the network is divided into clusters, the usage of hierarchical IDS schemes is suggested. Among the schemes presented in Table II, Su *et al.*'s [57] work is recommended, if the network is stable and no nodes are to be added. Otherwise, Bao *et al.*'s [72] work is suggested, as it is efficient for the scalable and dynamic network topologies.

For the researchers that are considering to simulate and compare the performances of the various IDS schemes, Adaobi *et al.*'s work [73] would be a good starting point. In their work, authors provide a case scenario on how to simulate an attack against a WSN and evaluate the performance of an anomaly-based IDS. Authors simulate their scenario in ns-2 simulation environment [74], with AODV protocol. They provide 4 metrics (namely, true positives, true negatives, false positives, and false negatives) calculated by analyzing the packet delivery ratio while changing the pulse rate.

To the best of our knowledge, there is no paper published regarding the effects of the IDSs on the energy consumption of WSNs. For the researchers that are considering to evaluate the cost of the IDS schemes on the WSNs, this would be a good topic to research.

VI. Conclusions

In this survey paper, IDSs along with their classifications, design specifications, and requirements are briefly introduced. Secondly, IDSs that are proposed for MANETs are presented and their applicability to WSNs are discussed. Thirdly, IDSs proposed for WSNs are discussed and their distinctive features are highlighted in a comparable chart, followed by the comments regarding IDSs that would be applicable to WSNs are presented. Finally, in order to help researchers in the selection of IDS for WSNs, recommendations of promising proposed schemes are provided along with future directions for this research.

TABLE III
List of abbreviations.

ARMA	autoregressive moving average
AODV	ad-hoc on-demand distance vector (routing)
BS	base station
CH	cluster head
DoS	denial of service
DSDV	destination sequenced distance vector
DSR	dynamic source routing
GPS	global positioning system
HIDS	host based intrusion detection system
IDS	intrusion detection system
IPS	intrusion prevention system
MANET	mobile ad-hoc network
NIDS	network based intrusion detection system
PCA	principal component analysis
UML	unified modeling language
WSN	wireless sensor network

VII. Acknowledgement

We would like to give special thanks to our colleagues Mr. David Donnelly, Dr. Dennis M. Parra, Ali Gorcin, Dr. Murad Khalid and Dr. Young-seok Lee for their reviews and valuable comments regarding the preparation and editing of this survey.

Last but not least, we would like to thank the anonymous reviewers for their valuable suggestions to improve the content and quality of our paper.

Appendix

Table III summarizes abbreviations used in this survey.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", *IEEE Commun. Mag.*, vol. 40, num. 8, pp. 102-114, 2002.

[2] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor network security: A survey", *IEEE J. Communications Surveys and Tutorials*, vol. 11, num. 2, pp. 52-73, 2009.

[3] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: a survey", *IEEE Commun. Surveys Tutorials*, vol. 10, num. 3, pp. 6-28, 2008.

[4] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", *book published by Wiley*, 2009.

[5] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Commun. Surveys and Tutorials*, vol. 8, num. 2, pp. 2–23, 2006.

[6] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *International J. Computer Science*, vol. 4, num. 1, pp. 1–9, 2009.

[7] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems", *Elsevier J. Information Security Technical Report*, vol. 10, num. 3, pp. 134-139, 2005.

[8] I. Butun and R. Sankar, "A Brief Survey of Access Control in Wireless Sensor Networks," *in Proc. IEEE Consumer Communications and Networking Conference*, Las Vegas, Nevada, January 2011.

[9] M. Ngadi, A.H. Abdullah, and S. Mandala, "A survey on MANET intrusion detection", *International J.Computer Science and Security*, volume 2, number 1, pages 1-11, 2008.

[10] Y. Zhang, W. Lee, and Y.A. Huang, "Intrusion detection techniques for mobile wireless networks", *J. Wireless Networks*, vol. 9, num. 5, pp. 545-556, 2003.

[11] I. Butun, Y. Wang, Y. Lee and R. Sankar, "Intrusion prevention with two–level user authentication in heterogeneous wireless sensor networks", *International J. Security and Networks*, vol. 7, no. 2, pp. 107–121, 2012.

[12] A. Patcha and J.M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", *Elsevier J. Computer Networks*, volume 51, number 12, pages 3448-3470, 2007.

[13] T.S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", *Elsevier J. Computer Standards and Interfaces*, volume 28, number 6, pages 670-694, 2006.

[14] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks", *Springer J. Wireless Network Security*, pages 159-180, 2007.

[15] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proc. 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1-12, April 2002.

[16] P. Michiardi and R. Molva, "Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," *Communication and Multimedia Security Conference (CMS'02)*, September 2002.

[17] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," *Proc. 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*, p. 57.1, January 2003.

[18] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez and E. Vazquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges", *Elsevier J. Computers and Security*, vol. 28, num. 1-2, pp. 18-28, 2009.

[19] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", *Proc. 1st ACM workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[20] A.P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz and H.C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," *in Proc. 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*, ACM Press, October 2005, pp. 16-23.

[21] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Ad Hoc Networks," *in Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks*, Orlando, FL, January 28, 2003.

[22] B. Sun, L. Osborne, Y. Xiao and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks", *IEEE Trans. Wireless Commun.*, vol. 14, num. 5, pp. 56-63, 2007.

[23] A.H. Farooqi and F.A. Khan, "Intrusion detection systems for wireless sensor networks: A survey", *Springer J. Communication and networking*, pp. 234–241, 2009.

[24] C.V. Zhou, C. Leckie and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", *Elsevier J. Computers & Security*, vol. 29, num. 1, pp. 124–140, 2010.

[25] H.T. Elshoush and I.M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems: A survey", *Elsevier J. Applied Soft Computing*, vol. 11, num. 7, pp. 4349–4365, 2011.

[26] C.V. Zhou, C. Leckie and S. Karunasekera, "Decentralized multidimensional alert correlation for collaborative intrusion detection", *Elsevier J. Network and Computer Applications*, vol. 32, num. 5, pp. 1106–1123, 2009.

[27] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel and M. Rajarajan, "A survey of intrusion detection techniques in Cloud", *Elsevier J. Network and Computer Applications*, vol. 36, pp. 42–57, 2013.

[28] K.A. Garcia, R. Monroy, L.A. Trejo, C. Mex-Perera,E. Aguirre, "Analyzing Log Files for Postmortem Intrusion Detection", *IEEE Trans. Syst. Man Cybern.*, vol. 42, num. 6, pp. 1690–1704, 2012.

[29] T.S. Cheng, Y.D. Lin, Y.C. Lai, P.C. Lin, "Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems", *IEEE Commun. Surveys Tutorials*, vol. 14, num. 4, pp. 1011–1020, 2012.

[30] G.Y. Keung, B. Li and Q. Zhang, "The intrusion detection in mobile sensor network", *IEEE/ACM Trans. Netw. (TON)*, vol. 20, num. 4, pp. 1152–1161, 2012.

[31] Y. Wang, W. Fu, D.P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, num. 2, pp. 342–355, 2013.

[32] E. Shakshuki, N. Kang and T. Sheltami, "EAACK– A Secure Intrusion Detection System for MANETs", *IEEE Trans. Ind. Electron.*, vol. 60, num. 3, pp. 1089–1098, 2013.

[33] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks", *Proc. 6th annual international conference on Mobile computing and networking*, pp. 275-283, 2000.

[34] O. Kachirski and R. Guha, "Intrusion Detection using Mobile Agents in Wireless Ad Hoc Networks", *IEEE Computer Society*, 2002.

[35] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs," *Proc. 3rd IEEE International Workshop on Information Assurance (IWIA'05)*, pp. 57-70, March 2005.

[36] R. Puttini, M. Hanashiro, F. Miziara, R. de Sousa, L. Garcia-Villalba and C. Barenco, "On the Anomaly Intrusion-Detection in Mobile Ad Hoc Network Environments", *in Proc. 11th IFIP TC6 international conference on Personal Wireless Communications*, Springer, pages 182-193, 2006.

[37] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited", *in Proc. IEEE GLOBECOM*, 2003.

[38] K. Nadkarni and A. Mishra, "Intrusion detection in MANETs-the second wall of defense", *in Proc. 29th Annual Conference of the IEEE Industrial Electronics Society*, 2003.

[39] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Adhoc NeTworks)," *Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02)*, pp. 226-336, June 2002.

[40] B. Sun, K. Wu and U.W. Pooch, "Zone-based intrusion detection for mobile ad hoc networks", *Int. J. Ad Hoc and Sensor Wireless Networks*, volume 2, number 3, 2003.

[41] A. Patcha and J.M. Park, "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks", *in Proc. IEEE Information Assurance Workshop*, 2004.

[42] A. Patcha and J.M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks", *International J. Network Security*, volume 2, number 2, pages 131-137, 2006.

[43] S. Sen and J.A. Clark, "Evolutionary computation techniques for intrusion detection in mobile ad hoc networks", *Elsevier J. Computer Networks*, vol. 55, num. 15, pp. 3441–3457, 2011.

[44] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *International Conference on Mobile Computing and Networking (MobiCom)*, pp. 255-265, 2000.

[45] F.H. Wai, Y.N. Aye, and N.H. James, "Intrusion Detection in Wireless Ad-Hoc Networks", 2003.

[46] M. Jahnke, A. Wenzel, G. Klein, N. Aschenbruck, E. Gerhards-Padilla, P. Ebinger and S. Karsch, "MITE-MANET Intrusion Detection for Tactical Environments", *in Proc. NATO/RTO IST-076 Research Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana, Slovenia, 2008.

[47] M. Wei and K. Kim, "Intrusion detection scheme using traffic prediction for wireless industrial networks", *IEEE J. Communications and Networks*, vol. 14, num. 3, pp. 310–318, 2012.

[48] A. Mishra, K. Nadkarni and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks", *IEEE Trans. Wireless Commun.*, pp. 48-60, 2004.

[49] S. Sen and J.A. Clark, "Intrusion detection in mobile ad hoc networks", *Springer J. Guide to Wireless Ad Hoc Networks*, pages 427-454, 2009.

[50] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *in Proc. IEEE Consumer Communications and Networking Conference*, 2006.

[51] Crossbow MICAz mote data sheet, cited in August 2012, available at: http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICAz_Datasheet.pdf

[52] Atmel ATmega128L microcontroller data sheet, cited in August 2012, available at: http://www.atmel.com/Images/doc2467.pdf

[53] Intel notebook processors, cited in August 2012, available at: http://www.intel.com/support/processors/mobile/pm/sb/cs-007967.htm

[54] XBee WiFi module data sheet, cited in August 2012, available at: http://www.digi.com/pdf/ds_xbeewifi.pdf

[55] S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks", *IEEE Trans. Ind. Informat.*, volume 6, number 4, pages 744-757, 2010.

[56] R.C. Chen, C.F. Hsieh, Y.F. Huang, "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", *in Proc. ACM ICUIMC-09*, 2009.

[57] C.C. Su, K.M. Chang, Y.H. Kuo and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", *in Proc. IEEE Wireless Communications and Networking Conference*, 2005.

[58] A.A. Strikos, "A full approach for intrusion detection in wireless sensor networks", *School of Information and Communication Technology*, 2007.

[59] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, "Distributed Anomaly Detection in Wireless Sensor Networks", *10th IEEE Singapore International Conference on Communication systems*, 2006.

[60] I. Krontiris, T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", *Proc. 13th European Wireless Conference*, 2007.

[61] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks", *Springer J. Wireless Sensor Networks*, pp. 263-278, 2009.

[62] E. Ngai, J. Liu and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *ICC'06*, Istanbul, Turkey, June 2006.

[63] S.S. Doumit and D.P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", *in Proc. IEEE Military Communications Conference (MILCOM'03)*, 2003.

[64] I. Onat and A. Miri, "A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks", *Proc. Systems Communications*, 2005.

[65] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," *Proc. 3rd IEEE International Symposium on Network Computing and Applications (NCA'04)*, pp. 343-346, 2004.

[66] A. Agah and S.K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach", International Journal of Network Security, volume 5, number 2, pages 145-153, 2007.

[67] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks", *IEEE Trans. Wireless Commun.*, 2008.

[68] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", *IEEE ICC '07*, Glasgow, U.K., June 2007.

[69] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. High Speed Networks*, vol. 15, no. 1, pp. 33-51, 2006.

[70] I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2005.

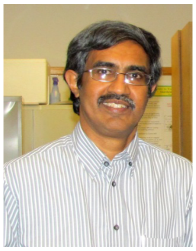
[71] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, num. 5, pp. 835–843, 2012.

[72] F. Bao, R. Chen, M.J. Chang and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", *IEEE Trans. Network Service Management*, vol. 9, num. 2, pp. 169–183, 2012.

[73] O. Adaobi, E. Igbesoko and M. Ghassemian, "Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-Organised Networks", *IEEE 5th International Conference on New Technologies, Mobility and Security (NTMS)*, 2012.

[74] The network simulator, ns-2, cited in January 2013, available at: http: //www.isi.edu/nsnam/ns/

İsmail Bütün (ibutun@mail.usf.edu) received his B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from Hacettepe University, Ankara, Turkey, in 2003 and 2006, respectively. He received his second M.Sc. degree in Electrical Engineering from University of South Florida in 2009. He is currently pursuing his Ph.D. degree in Electrical Engineering at University of South Florida. He is member of the Interdisciplinary Communications, Networking and Signal Processing (iCONS) Research group (http://icons.eng.usf.edu). His research interests are computer networks, network security and wireless communications. For further details, visit his web page: http://www.eng.usf.edu/∼ibutun



Ravi Sankar (sankar@usf.edu) received the B.E. (Honors) degree in Electronics and Communication Engineering from the University of Madras, the M.Eng. degree in Electrical Engineering from Concordia University and the Ph.D. degree in Electrical Engineering from the Pennsylvania State University. Since 1985, he has been with the Department of Electrical Engineering at the University of South Florida, where he is currently a USF Theodore and VenetteAskounes-Ashford Distinguished Scholar Award winning Professor of Electrical Engineering and Director of the interdisciplinary Communications, Networking, and Signal Processing (iCONS) research group. His main research interests are in the areas of wireless communications, networking, signal processing and its applications. For further details about his research and group, visit http://icons.eng.usf.edu.