Wireless Sensor Network, 2011, 3, 241-261
doi:10.4236/wsn.2011.37026 Published Online July 2011 (http://www.SciRP.org/journal/wsn)

A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable

Hossein Jadidoleslamy
Department of Information Technology, *Anzali International Branch*, *The University of Guilan*, *Rasht*, *Iran*
E-mail: *tanha.hossein@gmail.com*
Received May 23, 2011; *revised June* 2, 2011; *accepted June* 22, 2009

Abstract

Networks protection against different types of attacks is one of most important posed issue into the network and information security domains. This problem on Wireless Sensor Networks (WSNs), in attention to their special properties, has more importance. Now, there are some of proposed solutions to protect Wireless Sensor Networks (WSNs) against different types of intrusions; but no one of them has a comprehensive view to this problem and they are usually designed in single-purpose; but, the proposed design in this paper has been a comprehensive view to this issue by presenting a complete Intrusion Detection Architecture (IDA). The main contribution of this architecture is its hierarchical structure; *i.e.* it is designed and applicable, in one, two or three levels, consistent to the application domain and its required security level. Focus of this paper is on the clustering WSNs, designing and deploying Sensor-based Intrusion Detection System (SIDS) on sensor nodes, Cluster-based Intrusion Detection System (CIDS) on cluster-heads and Wireless Sensor Network wide level Intrusion Detection System (WSNIDS) on the central server. Suppositions of the WSN and Intrusion Detection Architecture (IDA) are: static and heterogeneous network, hierarchical, distributed and clustering structure along with clusters' overlapping. Finally, this paper has been designed a questionnaire to verify the proposed idea; then it analyzed and evaluated the acquired results from the questionnaires.

Keywords: Wireless Sensor Network (WSN), Security, Intrusion Detection System (IDS), Hierarchical, Distributed, Scalable, Dynamic Reconfigurable, Attack, Detection

1. Introduction

Wireless Sensor Networks (WSNs) are homogeneous or heterogeneous systems consist of many small devices, called sensor nodes, that monitoring different environments in cooperative [1,2], *i.e.* sensor nodes cooperate to each other and combine their local data to reach a global view of the operational environment; they also can operate autonomously. In WSNs there are two other components, called "aggregation points" (*i.e.* cluster-heads and CIDSs' deployment locations) and "base station" (*i.e.* the central server and the WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes [1,3]. As shown in **Figure 1**, aggregation points collect information from their nearby sensor nodes, aggregate and forward them to the base station to process gathered data [4]. Factors such as wireless, unsafe, unprotected and shared nature of communication channel, untrusted and broadcast transmission media, deployment in hostile and open environments, automated and unattended nature and limited resources, make WSNs vulnerable and susceptible to many types of attacks [1]; therefore, in attending to the WSNs' constraints, their requirements and unusable traditional network security techniques on WSNs, security is a vital and complex requirement for these networks [2,5]. Also, the defensive-security mechanism that can guarantee the normal functionalities of these networks must be consistent to the WSNs' autonomous mechanisms. This paper is following a complete security mechanism to cover and establish different basic security dimensions of WSNs, like confidentiality, integrity, availability and authenticity. Our proposal is adding an another defensive line, called Intrusion Detection System (IDS), as a new defensive-security layer to the WSNs' security infrastructure; which it can

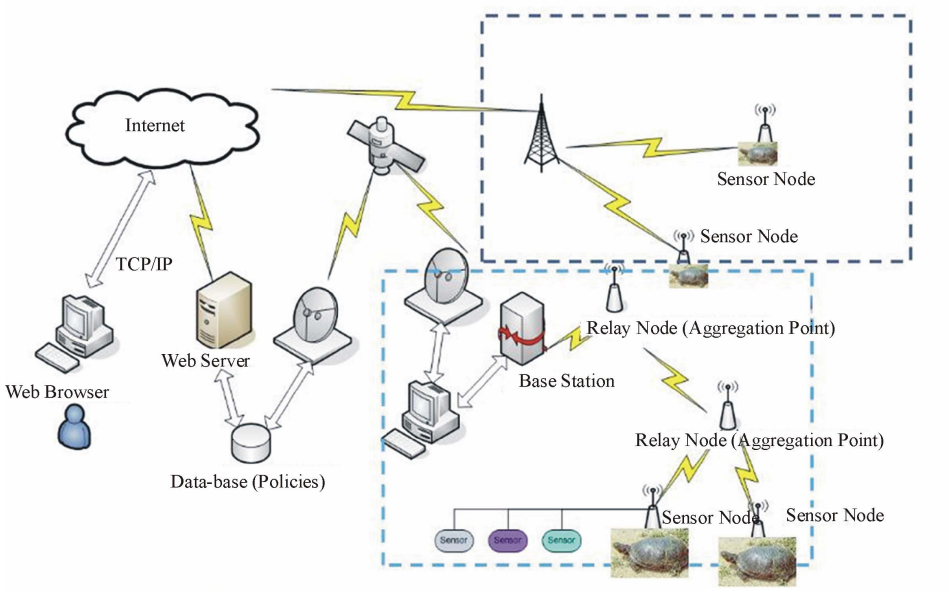


Figure 1. WSNs' communication architecture.

detects unsafe activities and unauthorized access; also, when attacks occurred, even new attacks such as anomalies, it can get notify by different warnings and perform required actions (mainly predefined actions). Therefore, the main purpose of this paper is presenting, discussing and solving the intrusion detection problem in WSNs. This paper is including:

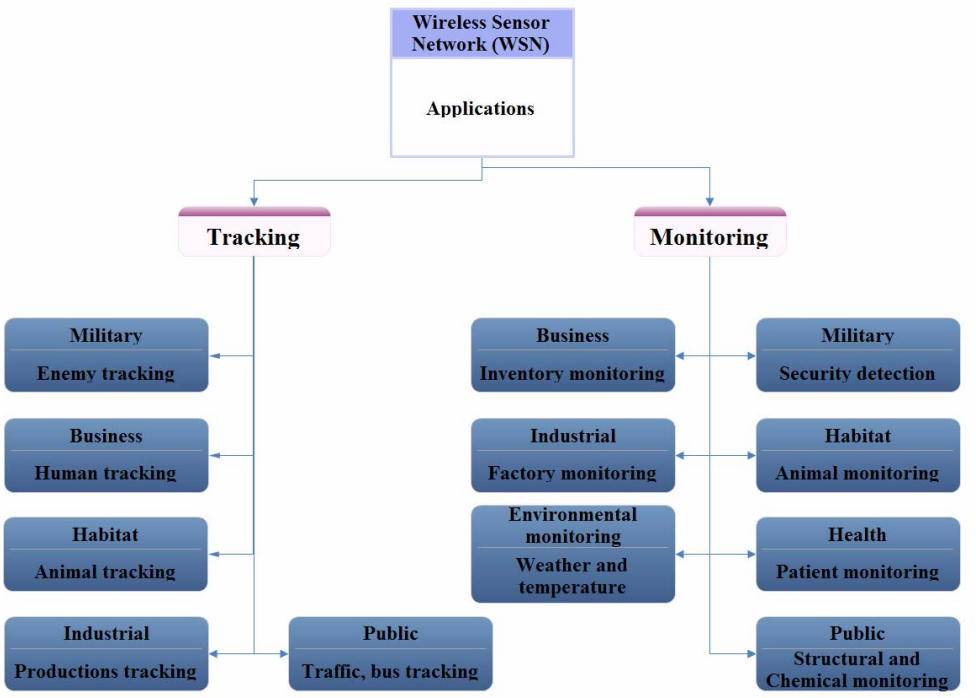
- An overview of WSNs and their security;
- Discussing Intrusion Detection System (IDS) as a new aggressive-defensive security layer for WSNs (consider the basic architecture of IDSs and IDS's requirements for WSNs);
- Suggestion a comprehensive, hierarchical and uncentralized Intrusion Detection Architecture (IDA) and IDS architecture for WSNs (SIDS, CIDS and WSNIDS architectures);

This paper makes us enable to identify the existent security challenges in WSNs and we can almost solve the intrusion detection problem on these networks; besides, we also can detect and manage WSNs' attacks and react to them, appropriate to attacks' type and their nature. The rest of this paper is organized as follows: in Section 2 an overview of WSNs and their different security dimensions are presented; Section 3 is mainly focused on IDS, it's importance and different dimensions, and IDS's required properties for WSNs; Section 4 considers the intrusion detection issue on WSNs, including design challenges and IDS requirements in these networks; Section 5 will describe the proposed Intrusion Detection Architecture (IDA) and suggested IDSs for WSNs; Section 6 prepares a questionnaire to verifying the IDA; it also expressed the reached results from analyzing questionnaires; Section 7 presented conclusion; and finally future works, are drawn in Section 8.

2. An Overview of WSNs

Sensor is a tiny device which detects and measures amount of physical parameters, or an event occurrence, or an object existence; then, it converts that value to electrical signal; finally, if necessary, it actuates a special operation by using electrical actuators [1,6]. WSN is a computer network with following major features:

- Infrastructure-less [1,2,3];
- No public address, often (data-centric network, thus sensor nodes do not have identification code) [2,7];
- Consists of many (hundreds or even thousands) tiny sensor nodes [2,8,9] (small size, low-cost and low-power);
- High-density of nodes distribution [3,10];
- Insecure radio links;
- Application-oriented;
- Central or distributed management;
- Different communication models [1,2,11], including: hierarchical/distributed WSNs or homogenous/heterogeneous WSNs;
- Limited resources of sensor nodes [2,3,12] (radio communication, bandwidth, energy, memory and processing capabilities) [7,10,13];
- Having decision making capability to react to the events, including: automated structure (local decision making), semi-automated (decision making by base-station) and combinational (clustering structure);
- Main application domains of WSNs are: monitoring and tracking (as shown in following figure, **Figure 2(a)**); therefore, some of the most common applica-



(a)

(b)

Figure 2. WSN's applications.

tions of these networks are: military, medical, environmental monitoring, industrial, infrastructure protection, disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery (as shown in **Figure 2(b)**).

The taken approach into the WSN is a combinational model; *i.e.* hierarchical, distributed and heterogeneous; since, sensor nodes, cluster-heads and the central server are different than each other and each one of them have special and different capabilities, hardware and software specifications than others.

In continue of this section, it will be presented an outline of different aspects of WSNs, such as their characteristics, vulnerabilities and different security dimensions.

2.1. Vulnerabilities and Challenges of WSNs

WSNs are vulnerable against many kinds of attacks; some of the most common reasons are:

- Theft [1] (reengineering and replicating) [3,5];
- Limited capabilities and resources [2,5];

- Random deployment [7];
- Deployment on dynamic/hostile environments [2,10];
- Insider attackers;
- Inapplicable traditional network's common security techniques [2,5] (due to limited devices and their resources and interaction to physical environment);
- Requirement to redesigning security architectures and protocols (distributed and self-organized);
- Unreliable communications [2] (connectionless packet-based routing ⇨ unreliable transfer, channel's broadcast nature ⇨ conflicts, multi-hop routing and network congestion and node processing ⇨ Latency);
- Vulnerability against eavesdropping (since using unique communication frequency into the WSN);
- Unattended nature and operation [1,2];
- Dynamic structure, unpredictable topology and self-organization [1,3];
- Sensor nodes' selfishness [2,12];
- Requiring to forwarding and routing sensed information to a shared destination, called sink;
- Existence redundancy in gathered traffic;
- Fault tolerant [1,12];
- Cost of sensor nodes' development and their production [2,6];
- Size and precision of sensor nodes;

2.2. Security in WSNs

As WSNs' application areas are growing, intrusion techniques in these networks also are increasing; there are many methods to disrupt these networks and every day, new techniques are representing to destruct WSNs [1,2]. Besides, in attending to the vital WSNs' vulnerability against many types of attacks [5,11] and necessity of data accuracy and network health and fault tolerant, confidential and sensitive applications of WSNs, security is a vital requirement in these networks and it must be established according to their constraints to can solve security problems and weaknesses of these networks. Also, there are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). Thus, security in WSNs is an important, critical issue, necessity and vital requirement, due to:

- Correctness of network functionality [1,2];
- Unusable typical networks protocols [2,7];
- Limited resources and untrusted sensor nodes [1,8];
- Requiring trusted center for key management, to authenticate nodes to each others, preventing from existent attacks and selfishness [1,10,13] and extending collaboration [2];
- Broadcast and wireless nature of transmission media [1,5];
- Sensor nodes deploy on hostile environments [1,6,12] (unsafe physically);
- Unattended nature and operation of WSNs [1,2,9];

Some of most important dimensions of WSNs have been shown in following figure (**Figures 3(a) and (b)**) by star spangled. As **Figure 3(a)** shows, in this paper we have emphasize on goals, obstacles and constraints of WSNs' security aspects. Also, **Figure 3(b)** is showing which this paper has been emphasized on intrusion detection approach from security mechanisms (by star spangled).

3. Intrusion Detection System (IDS)

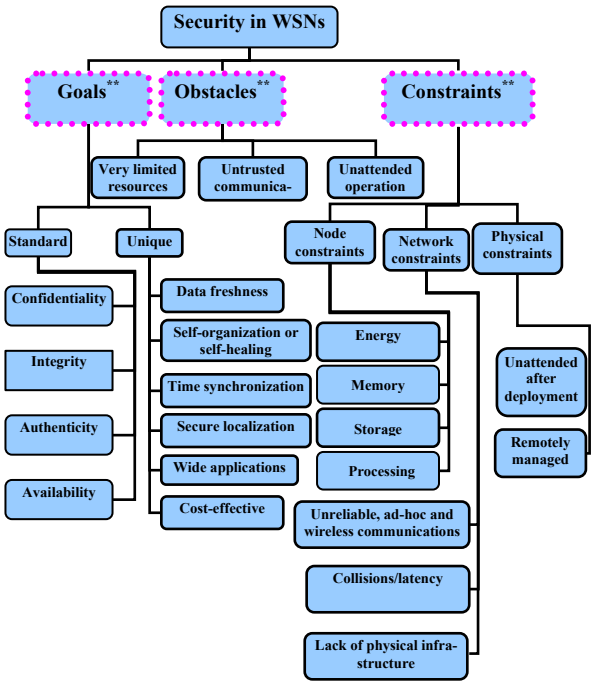
Intrusion, *i.e.* unauthorized access or login (to the system, or the network or other resources) [14]; intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network's resource [15,16]. Intrusion detection is a process which detecting contradictory activities with security policies to unauthorized access or performance reduction of a system or network [14]; the purpose of intrusion detection process is reviewing, controlling, analyzing and representing reports from the system and network activities. Intrusion Detection System (IDS), *i.e.*:

- A hardware or software or combinational system, with aggressive-defensive approach to protect information, systems and networks [17,18];
- Usable on host, network [19] and application levels;
- For analyzing traffic, controlling communications and ports, detecting attacks and occurrence vandalism, by internal users or external attackers;
- Concluding by using deterministic methods (based on patterns of known attacks) or non-deterministic [18, 19] (to detecting new attacks and anomalies such as determining thresholds);
- Informing and warning to the security manager [16, 17,20] (sometimes disconnect suspicious communications and block malicious traffic);
- Determining identity of attacker and tracking him/her/it;

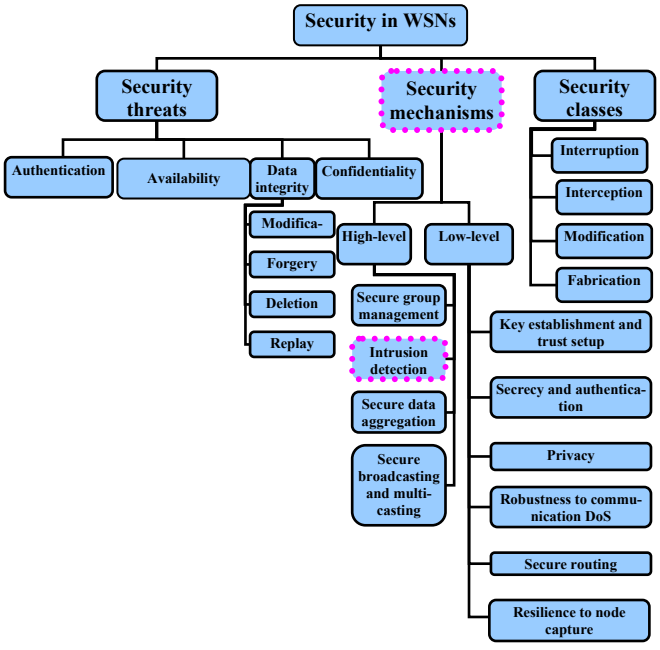
There are three main functionalities for IDS, including: monitoring (evaluation), analyzing (detection) and reacting (reporting) [15,17] to the occurring attacks on computer systems and networks. If IDS be configured, correctly; it can represent three types of events: primary identification events (like stealthy scan and file content manipulation), attacks (automatic/manual or local/remote) and suspicious events.

3.1. IDS Categorization Based on Their Architecture

According to the **Figure 4**, Intrusion Detection Systems



(a)



(b)

Figure 3. Security in WSNs.

(IDSs) attending to the information gathering source and input data supplier, divide into three categories, as follows.

3.1.1. Host-Based Intrusion Detection System (HIDS)

HIDS installs on a computer system [15,18]; it uses processor and memory of that system and protects only the hosting system [15,21]. It has an abnormal detector part which using statistical methods to detect abnormal behavior of users in comparison to their behavioral records [21,22]; also, it has an expert system part that detects the security threats and describes the vulnerabilities of the system, but independent from behavioral records of users; of course, it uses a rules-base, too.

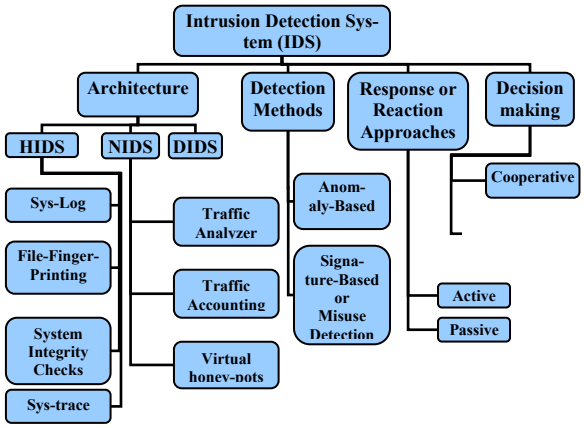


Figure 4. Different categorizations of IDSs.

3.1.2. Network-Based Intrusion Detection System (NIDS)

NIDS is a software process which installs on a special hardware system [16,20]; in many cases, it operates as a sniffer and controls passing packets and active communications, then it analyzes network traffic in sophisticated, to find attacks [18,19,22,]. NIDS can identify attacks, on network level; thus, it includes following steps:

- Setting up the Network Interface Card (NIC) on promiscuous mode and eavesdropping total network traffic [16];
- Capturing the transmitting network packets [19];
- Extracting requirement information and properties from them (the packets);
- Analyzing properties and detecting statistical deviation from normal behavior and known patterns (using pattern matching);
- Producing and logging proper events;

3.1.3. Distributed Intrusion Detection System (DIDS)

Most important characteristics of DIDS are:

- Combination of HIDS, NIDS and central management system [23];
- Sending the reports of distributed IDSs (HIDSs and NIDSs) to the central management system;
- Based on distributed and heterogeneous resources [14,15,20];
- High complexity, variable specifications and agent-based.

In WSNs, most attackers are targeting routing layer, since they can control passing information into the network. Besides, WSNs mainly are based on sensor nodes' reporting to the base station; so, disrupting and violating from this process leads to success attacks. As a result, for such networks, most proper architecture for IDS will be NIDS. A NIDS using network raw data packets as data source; it eavesdrops and listens to the network traffic, captures packets in real-time, then controls and tests them to detect attacks.

There is a SIDS on each sensor node to detect attacks on sensor-level wide; mainly, physical attacks. Also, in the proposed architecture, sensor nodes are partitioned as some clusters; each cluster has a cluster-head and any cluster-head (CIDS) should monitor the traffic of its associated cluster nodes. But, in some cases (about boundary nodes), a single cluster-head can not solve the "trust no node" requirement; thus, neighboring and corresponding cluster-heads have to cooperate to each others to complete the intrusion detection process. They can use the simple majority vote rule to make an appropriate decision. In other cases, a human agent or the WSNIDS (deployed IDS on the central server) is completing the intrusion detection process.

3.2. IDS Classification Based on Detection Method

IDSs must be able to differentiate between normal and abnormal activities, to detect malicious efforts, in real-time. As **Figure 4** shows, IDSs be partitioned into two categories, based on data analysis and detection method [15,17]. In following sections, they will be considered.

3.2.1. Anomaly Detection Systems

Anomaly Detection Systems are focused on normal behavioral patterns [18,20]. According to the expert systems are not able to timous update patterns, we will need automatic devices to extract new attacks' patterns [14, 15,20]. It is possible to using some techniques such as threshold detection (fully heuristic and static), statistical criteria, act/rule-oriented criteria, clustering methods, neural networks, expert systems, machine learning and data mining, to detecting abnormal behaviors [12,24]; for example, measuring the changes in volume, direction and pattern of communication traffic, can indicate and differentiate attack traffic, easily. In this approach, it is possible to detecting new attacks and also internal attackers; including following steps:

- Identifying normal behaviors [20,22] (they have deterministic properties) and finding especial rules for them (describing normal behaviors by automated learning, usually);
- Forming some views from normal behaviors of the system, network, users and user groups;
  - Behaviors that following these patterns ⇨ normal behaviors;
  - Activities which have excessive deviation from defined statistical values of these patterns ⇨ abnormal behaviors and intrusion efforts;

The main key to detect abnormal behavior: comparing current traffic and predefined normal behaviors patterns;

Problem: how gathering a set of static criteria of normal behaviors?

3.2.2. Signature-based Detection Systems

This method is using deterministic scenarios, rules and patterns of known attacks, which be defined by security expert systems, to detect security threats and attacks [17, 24]; in this model, IDS gathers the properties of attacks and abnormal behaviors and then, make an information base by them [18,20,22]. Therefore, to using such systems, user should define and store the templates and requirements actions for security threats. After pattern and properties matching, IDS can report the type of attack, in precise. Thus, the main operation of these systems is comparing observed behavior and known attacks' patterns to each other. Some of characteristics of this approach are:

- Inability to identifying new attacks [15,20];
- Requiring to a set of predefined patterns [17,24] (including properties, rules and behaviors) of known attacks into the IDS;
- Necessity of adding new patterns of attacks to the patterns' set, manually and repeatedly;

The main key to detect misuse behavior: comparing current traffic to predefined and pre-known attacks' patterns;

Problem: how detecting intrusions' properties and displaying them?

In attending to the surveys conducted, severe restrictions of resources on WSNs, especially memory, using of such IDSs which requiring storing the patterns of attacks, they are not usable or rather difficult to using on WSNs.

Proposed detection approach on the WSN is combinational method (specifications-based); *i.e.*, based on signature and based on anomaly. In this approach, at first, defining manually some of deterministic properties and thresholds of normal behavior for the system; thus, deviation of them, is anomaly. This system can be had two types of policy-bases, including: Misuse-detection policy-base and Anomaly-detection policy-base.

Proposed detection method is uncentralized; because IDSs are distributed and installed on different levels of the network: the WSNIDS on the central server (highest level), CIDSs on cluster-heads (medium level) and SIDSs on sensor nodes (low level). Distributed systems are more scalable and more robust; since they have different views of the network. Besides, IDS can inform the occurrence of attacks, in fast; because the network is clustering, SIDSs and CIDSs are distributed as cover total nodes of the network; then, SIDSs and corresponding CIDSs are near to the attackers (on single hop distance).

It is possible to detect in 1, 2 or 3 levels; *i.e.* if SIDS can not detect attack or make decision about attack occurrence or its policy-base does not have the pattern of the type of a special attack, the SIDS is tagging that packet and then, send it to the high-level IDS (*i.e.* corresponding CIDS); if the CIDS can not detect attack or make decision about attack occurrence or its policy-base does not have the pattern of the type of a special attack; the CIDS is labeling that packet and then, send it to the high-level IDS (*i.e.* WSNIDS); now, WSNIDS should make final decision if the current traffic is malicious or not.

3.3. IDS Categorization Based on Decision Making Techniques

In this section, the paper discusses about who should make final decision if occurring intrusion or not, or if a node is an intruder, really? Is an attack accrued? If ok, what actions must be doing? According to the **Figure 4**, there are two approaches for this purpose, as follows.

3.3.1. Cooperative Mechanism

In a cooperative IDS, if a node detects an anomaly, or the existent evidences be inconclusive, a cooperative mechanism triggers to produce a global intrusion detection action along with neighboring nodes; even if a node be sure about the crime of another node, decision making also should be cooperative (again) [17,20]; because the node which take the decision, maybe be malicious, itself. Besides, for decision making about boundary nodes between neighboring clusters in the network wide level, corresponding cluster-heads (using collector and majority rule), and if necessary, the central server (WSNIDS), should take proper decisions by participate to each other.

3.3.2. Autonomous Mechanism

In this method, sensor nodes and cluster-heads take decisions, autonomously [15,21]; they gather evidences and criteria of anomaly and intrusion activities from co-cluster nodes and then, make decision on sensor-level or cluster-level intrusions. Other nodes, clusters and the WSNIDS, do not have cooperated in this decision making process. The main weaknesses of this approach are:

- Security of sensor nodes and cluster-heads is low [17,25] (of course, in homogenous WSNs); attackers can compromise them soon and easy; therefore, this leads to loss of the network control.
- Enforcing excessive processing overhead on cluster-heads; therefore, in attending to limited resources and being few key nodes, on homogenous WSNs, leads to their lifetime reduction (energy loss/waste

and cluster-heads destruction). Processing the information of other nodes and then, taking appropriate decision on results of intrusion efforts (if leads to an attack or not), enforcing excessive processing overhead and finally, can be leading to energy loss/waste and exhaustion of decision maker nodes (cluster-heads).

The proposed IDA for WSNs, can take combinational decision making approach (autonomously, but often cooperative) by using clustering manner; thus, SIDSs make decision about intrusion occurrence on sensor node level; if necessary they referenced to the corresponding CIDSs; also, cluster-heads make decision about intrusion occurrence and proportional actions on cluster level; if necessary, they cooperate to each others (for example, about boundary nodes). *i.e.*, the WSN's nodes be clustering and forming clusters; in each cluster, sensor nodes collect data from environment, cluster-heads gather data from corresponding cluster's nodes, then form and maintenance a machine state for any one of them; then, cluster-head (CIDS) can take proper decision if the node be compromised or not; or if any node disclosure information or not; of course, by attention to the nodes' reports. Therefore, in each cluster, SIDSs make decision on intrusion to the local host nodes; also, corresponding cluster-head make decision on intrusion to its co-cluster nodes. So, in some cases (about boundary nodes), neighboring cluster-heads cooperate to each other to detect intrusions. Besides, in cases of anomaly detection, special attacks or inapplicability majority rule, the central server (WSNIDS) or human agents make final decisions about attack occurrence and proper reactions.

In suggestion approach, at first level, sensor nodes make decision on attack occurrence to local host sensor node; at second level, cluster-heads make decision on attack occurrence to associated clusters' sensor nodes and then, cluster-heads of boundary nodes cooperate to each other about intrusion occurrence and proportional actions (cooperative decision making); finally, the WSNIDS take decision on anomalies and difference cases between cluster-heads.

We can establish a combinational decision making mechanism by using this actual that whole sensor nodes deploy in associated cluster-heads and the WSNIDS radio range; also, cluster-heads deploy in each other and the central server (WSNIDS) radio communication range; it means that cluster-heads (to each other) and WSNIDS have communicate to each others; thus, each cluster-head can listen to the transmitted messages of its neighboring cluster-heads and the WSNIDS. Therefore, these nodes can advertise their warnings to each other, easily; through produce and broadcast a single message. In suspicious cases of boundary nodes can have a safer and more reliable conclusion by using the majority rule:

"If more than half of a node's corresponding cluster-heads warn, then that node is a compromised node and it should be turning off or the central server must be notified and take proper decision about it".

It means, if a boundary node has been n corresponding cluster-heads, if the collector receives at least ((n/2) + 1)) warnings, also include the warning of the collector (itself), it can conclude which that node is a compromised node. Therefore, in cooperative approach, we have to select one of associated cluster-heads as collector, to gather warnings and ideas of other associated cluster-heads and enforce the majority rule; then, the final conclusion and decision making do by collector.

For enforcing the majority rule, we have to determine a cluster-head as collector, to gather warnings from other cluster-heads analyze them and take the final decision.

Problem 1: compromising collector: attacker can control intrusion result, easily. To avoid from this scenario, other cluster-heads must impose the majority rule on the received warnings, too; then, they have to check, consider and compare reached result to the collector's report.

Problem 2: compromising a few cluster-heads: in attending to majority rule, if a cluster-head compromised and broadcasts a false warning, and tries to cancel an authorized node or does not broadcast a warning for a malicious node; this is almost ineffective; because most of cluster-heads are win and non-compromised, yet.

3.4. IDS Categorization Based on Response Method

IDSs using events' information and patterns analysis of attacks to react them; including:

3.4.1. Active Response

These responses prevent from the attackers' activities, directly [13,16]; for example, session disconnection [19], dynamic reconfiguration of the network, using Honeypot and setting thresholds again (in attention to the user skill, network speed, expected network connections, work load of security manager, sensor sensitivity, security policy, vulnerabilities, information and system sensitivity and fault importance).

3.4.2. Passive Response

These kinds of responses do not prevent from the attackers' activities, directly [15,17,18]; like: shunning, logging, notifying [15] through cell phone, email and message to SNMP console [18,20].

The proposed response approach for the WSN: using combinational method; *i.e.* active and passive responses by each others, depending on conditions, type and nature

of attacks; thus, the type of response be determining based on attacks' severity and their damages level. Also, responses can be as a part of policies; *i.e.* we can define and store responses into the info-bases such as Policy-base, manually.

4. Intrusion Detection on Wireless Sensor Networks (WSNs)

Intrusion detection in WSNs has many challenges, mainly due to lack or weak of resources [7,17]. Besides, the existent methods and protocols of traditional networks can not be enforced to the WSN, directly; because they need to the resources which attending to the WSNs' limitations and constraints are inaccessible. In general, WSNs are application-oriented [9,25]; *i.e.* they are designed as cover the very special properties according to the target application domain. Intrusion detection process is supposing that the behavior of normal system is differentiating than the behavior of attacked system. There are several possible and different configurations for WSNs; so, it is difficult to define normal and expected behavior; since the proposed IDS should have been different characteristics on different application domains.

Non-existence the unique structure for WSNs ⇨ Non-existence unique IDS ⇨ different and variety IDSs requirement ⇨ requiring to a modular and comprehensive IDS. For example, one of intrusion detection methods is checking, considering and distinguishing the running code on the sensor node; then, if it be differentiate than the normal code, it means which an attack is occurred or occurring [14,16].

4.1. Main Challenges in Designing IDS for WSNs

There are a lot of challenges in designing IDS for WSNs; as follows described:

- Designing efficient software to store and install on the sensor nodes, cluster-heads and the central server, to saving existent energy consumption; as a result, leading to increase the network lifetime;
- Limited resources [1,7,13,17];
- Repeated failures and unreliable sensor nodes;
- Application-oriented networks [11];
- Requiring to the monitoring, detecting, decision making and responding to the intrusions, in real-time and fast; then leading to minimum damages;
- It is difficult to time synchronizing nodes into the WSNs; so, it is difficult to using protocols that are rely on time synchronization;
- Databases challenges: the volume of sensed data in the dynamic and mobile WSNs; proper storage medium; supporting different queries from sensor nodes, cluster-heads and the central server in network wide level; data indexing and local queries to perform queries faster; indexing the mobile data; enforcing very costs by fast and real-time changes and communications and weak of data freshness (high-frequency of data freshness);

4.2. The basis Requirements of IDS on WSNs

In this section, the paper be described the basis requirements of IDS for WSNs; *i.e.* it wants to discuss the basis requirements of an IDS, which it has to provide for WSNs. Attacker can load the malicious software to trigger an internal attack, in attending to the special properties of these networks such as limited communication and processing resources, low radio range and other weakness of sensor nodes [11,25]. Therefore, an optimal and appropriate solution to solving this problem is architecture by following properties:

- Distributed;
- Based on cooperation of nodes, cluster-heads and the central server;

Then, a distributed and cooperative architecture is an optimal and proper solution. So, it is necessary which a WSNs' IDS has been following features:

- Localize auditing: IDS of WSNs should operate by using local and minor auditing data (such as SIDS, in the same sensor node level or CIDS, in the same cluster level); thus, distributed approach for these networks is appropriate and consistent (an accurate and comprehensive monitoring in sensor node level or cluster wide level, preprocessing, analyzing and processing).
- Accurate management of resources: IDS for WSNs has to consume minimum dose of nodes' and other network's resources (light-weight IDS). Besides, wireless networks do not have stable connections; also, the WSN's equipments and resources such as bandwidth and power, are limited. For example, the inter-nodes communications for intrusion detection purposes should not consume and occupy the accessible bandwidth, excessively.

Some of necessities are: non-enforcing extra load to the WSN, efficiency and monitoring the health state of IDSs.

- Error management, health state monitoring and security management: an IDS can not suppose that any single node is fully secure (supposition: no node is secure); because sensor nodes are compromising easily and disclosure information. Thus, in cooperative approaches, we have to attend that no nodes can be fully trusted.
- Accurate and comprehensive monitoring: data gath-

ering and analyzing them doing at some of specific location (such as cluster-heads).

Some of necessities are: non-enforcing extra load to the special components such as sensor nodes or cluster-heads into the WSN, using detection mechanism, audit trial, warning dependence, distributed and collective response at the level of the whole WSN.

- Robustness and fault tolerant: IDS must be robust and resistant against attacks [17,20]. Compromising one or more sensor node (their associated SIDSs) or even a cluster-head and controlling the behavior of its embedded CIDS, should not able attackers to remove an authorized node from the WSN or prevent from detecting another attacker or malicious node.

Some of necessities are: error management, keeping configuration information and security management.

- Secure and under-control inter-modules (internal parts of IDSs) and inter-components (between the WSN's components on different levels) data communications;
- Scalability;
- Reaction and tracking capabilities;
- Ease of use;

4.3. Intrusion Detection Approaches on WSNs

There are two major approaches for intrusion detection in this domain, as follows:

- Centralized approach: for applications with accessible nodes and possible to manage them, in centralize [15, 18]; but, this kind of architecture threats the entire system security.
- Distributed approach: in this approach, it is possible to have one IDS per each sensor node (SIDS); so, sensor node usually makes decision autonomously about sensor node level's attacks (mainly, physical attacks); also, there is one IDS per each cluster of nodes (CIDS); in this case, cluster-heads usually make decisions autonomously and independently about their associated and co-cluster sensor nodes; in some cases about boundary nodes, they cooperate to each others for intrusion detection; so, they take decisions, cooperatively. Thus, they using a cooperative mechanism to take proper decisions and then, they combine the local view of neighboring cluster-heads to each other. In clustering method, all cluster-heads that place in the radio range of a node, can surveillance on that node, to identify malicious nodes accurately by using the majority rule; even though chaining destruction.

The proposed approach is combinational; *i.e.* at first, the existent sensor nodes be classified in subsets, called cluster; then, a cluster-head be selected per each cluster. Now, in low level, a series of distributed IDS, called SIDS, be installed on sensor nodes; in medium level, a series of distributed IDS, called CIDS, be installed on cluster-heads; these IDSs have communicate to each other and corresponding cluster nodes; also, they have communicate to the central server (high level IDS: WSNIDS). Besides, there is a centralized and comprehensive IDS on highest level of the WSN intrusion detection architecture which has been installed and deployed on the powerful central server, calling the WSNIDS.

5. The proposed Intrusion Detection Architecture (IDA) for WSNs

As **Figure 5** is showing, the suggested architecture has a combinational (distributed, in two low levels and centralized, in highest level) and hierarchical structure; thus, the proposed approach can be used in 1, 2 or 3 levels of IDSs, including SIDSs (on sensor nodes), CIDSs (on cluster-heads) and the WSNIDS (on the central server).

5.1. Sensor-Based Intrusion Detection System (SIDS: Sensor Node Level IDS)

In low level of the proposed architecture (sensor nodes), there is a simple IDS or Sensor-based IDS (SIDS/HIDS) per each sensor node. In each sensor node, there is a small policy-base that is including most common attacks in this domain along with special and limited preprocessing capabilities such as extracting the required data fields from the network packet. This IDS is signature-based; if an attack be detected, according to the determined response into the corresponding policy and security rule, it be responded (autonomous and independent decision making). If the traffic was not on intrusion or there is not a matched policy in the sensor-based pol-

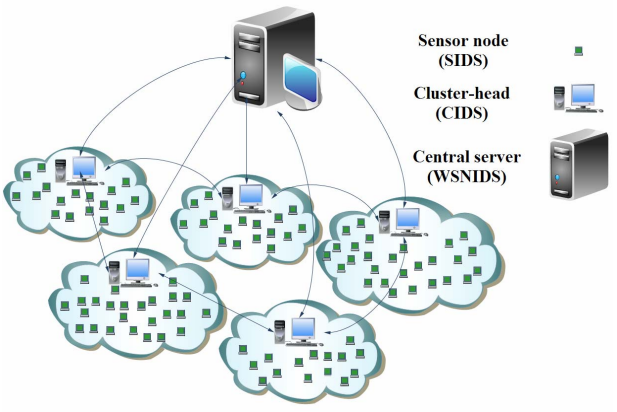


Figure 5. The proposed Intrusion Detection Architecture (IDA) for WSNs.

icy-base (SBPB), it be labeled and it will be send to the high-levels of the IDA (other IDSs) (cooperative deci--sion making), to considers more. Some of most important features of SIDS are:

- There is a SIDS on each typical sensor node; so, in this case, nodes besides performing the common functions of typical sensor nodes like sensing and gathering information, routing packets into the WSN and retransmission, doing also intrusion detection functionalities (operating as IDS, too).
- Architecture: HIDS;
- Detection method: signature-based;
- Response approach: hybrid;
- Decision making: almost independent and autonomous;
- Some of common operations of each SIDS are: preprocessing, extracting the properties and fields of packets, processing, enforcing rules and comparing policies to the current traffic by attending to the application area, type and nature of the WSN and possible attacks, decision making and finally, reacting by proper actions;
- Fields of data packets must be selected as be integrated, unique and low-size and low volume; besides, they should be optimal on processing, energy consumption, response time and delay; to leading to high performance. Some of most important fields are: Source: node-id, Next hop, Previous hop, Data type, Destination (CIDS/WSNIDS-id), Data and Sequence number (optional).
- SIDSs mainly are focused on detecting physical attacks of WSNs;
- Gathering data in intervals times, comparing them to the predefined thresholds and assigning a state label to them such as notification, warning or normal;
- In this approach, in attending to the distributed design for intrusion detection on WSNs, each sensor node only operates by using accessible local and partial information on the sensor node level; of course, it also using a distributed design for intrusion detection.
- In homogenous WSNs, SIDSs are same exactly on entire sensor nodes; they can broadcast, eavesdrop and listen to the messages (for example, messages that come from other neighboring sensor nodes). The communication between nodes, cluster-heads and the central server, provide possibility of using a distributed mechanism to take the final decision about intrusion threat.
- In heterogeneous WSNs, SIDSs are different than each others (since the systems and data types are different).
- The main properties of SIDSs are:
  - Using local and minor information for intrusion detection (localize auditing);
  - Low error rates;

Each sensor node in the WSN should have been a SIDS by following functionalities (according to **Figure 6**):

- Network monitoring: each sensor node monitors its immediate neighboring and nearby nodes to gathering audit data;
- Decision making: sensor node using gathered audit data (on previous step) to make decision on intrusion threat level based on node and appropriate responses; if necessary, it shares its findings with associated cluster-head (s) to take proper decision, in collective.
- Reaction: each sensor node has responding mechanisms which allow it to react to the intrusion situations.
- Internal components and modules which are existing into the SIDS's architecture are (as shown in **Figure 6**):
- local packet monitoring: gathering, auditing and filtering raw data for local detection engine module; these data usually are gathering by listening to the operating environment and transmissions of neighboring nodes (in promiscuous);

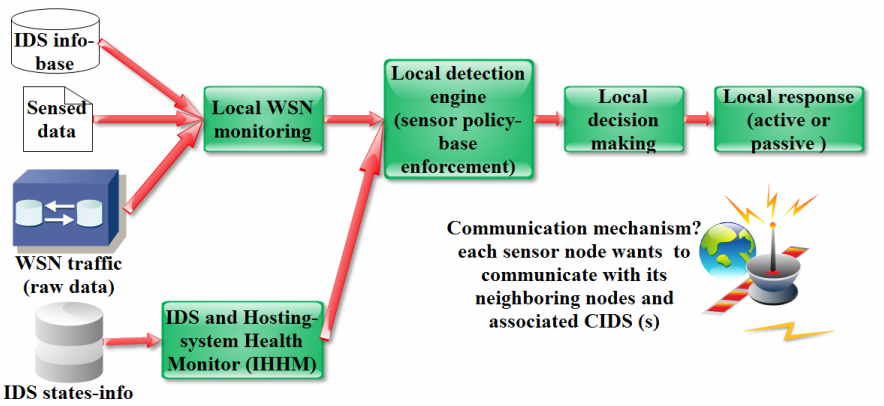


Figure 6. High-level architecture of the SIDS.

- Independent and local detection engine: analyzing and comparing audit data, in attending and considering to the properties, given limitations and predefined rules and enforcing detection techniques; this component stores, imposes and operates rely on signature-based detection method which describes attacks' patterns;
- Local decision making;
- local response module: it is possible to divide responses into two categories, according to the attacks' nature; *i.e.*: direct response and indirect response; once an intrusion occurred, compromised node will be detected and this module will trigger proper actions; including: disconnecting session, isolating intruder and compromised node, preventing the malicious/suspicious node from entire network's routes, network recovery, improving the used routing protocol, producing and using new cryptography keys, notifying to the associated cluster-head (s), reducing the quality estimation of the link to that node. According to the independent and autonomous behavior of WSNs, these functions must be doing without human agent intervention and in finite time.

Communication mechanism: this module is using to establish communication between sensor node (SIDS), cluster-heads (CIDSs) and the central server (the WSNIDS).

5.2. Cluster-Based Intrusion Detection System (CIDS: Cluster-Level IDS)

CIDSs place on the medium level of the proposed architecture (according to the **Figure 7**); *i.e.* they install and deploy on the heterogeneous cluster-heads. There is a cluster-head per each cluster of sensor nodes which it covers its radio range sensor nodes; so, the intrusion detection process does by cluster-heads. There is a small and low-size policy-base (Cluster-Based Policy Base: CBPB) on each cluster-head that includes the most common patterns of attacks on this domain, along with some preprocessing capabilities such as requirement data field extraction from the network packets and packets filtering. If an attack detects, according to the predefined actions into the policy-base and the corresponding security rule-base, the IDS is responding to it. In this level, decision is making in combinational; so, if the current traffic be from the internal of the cluster, the proper decision takes autonomously and independently; also, if the current traffic be from the boundary nodes (between different neighboring clusters), the collector be selected and then, the collector enforces the majority rule to takes the final decision; finally, if the current traffic not be about an intrusion or the collector can not take a decision (if the majority rule be inefficient), for more consideration, that traffic labeled (for example, rely on the attack esti-

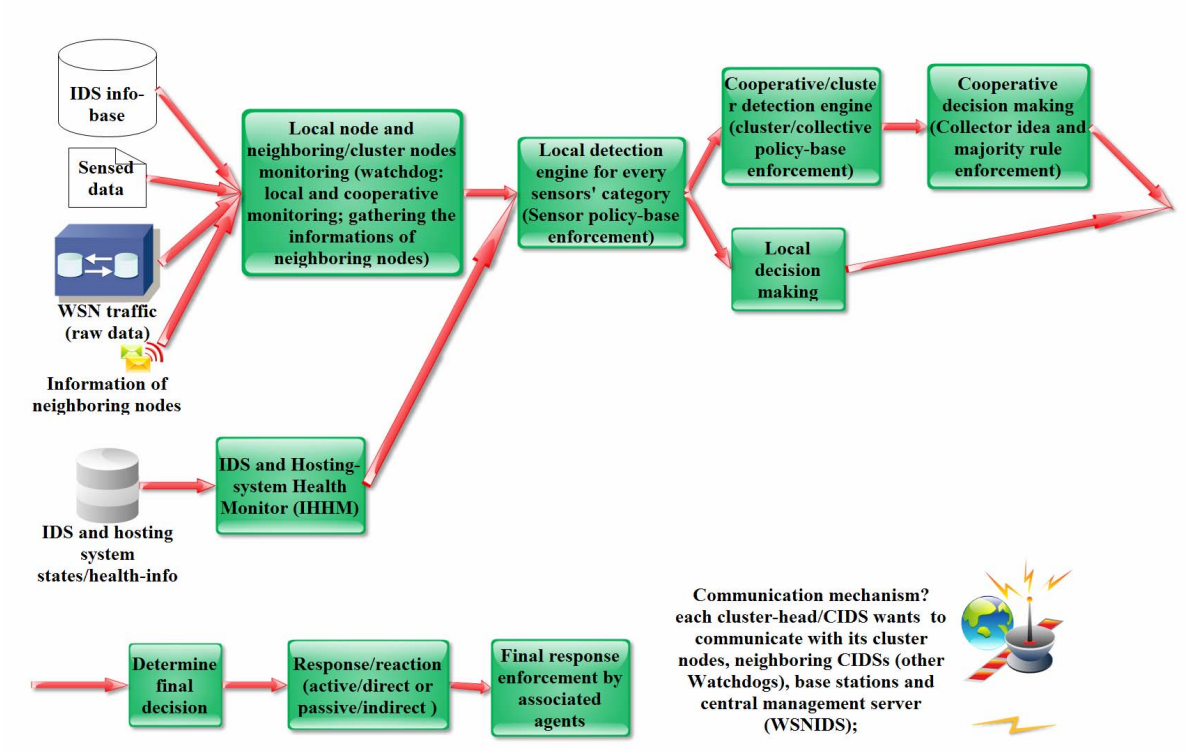


Figure 7. High-level architecture of the CIDS.

mation severity by current node) and will forward to the central server (centralized-cooperative decision making by CIDSs and the WSNIDS). Some of most common properties of CIDS are:

- A cluster-head node, besides performing the common functions of typical sensor nodes like sensing and gathering information, routing packets into the WSN and retransmission, doing also intrusion detection functionalities.
- Some of common operations of each CIDS are: pre-processing, filtering, reducing unsuitable data, extracting the properties and fields of packets, processing, enforcing rules and comparing policies to the current traffic by attending to the application area, type and nature of the WSN and possible attacks, decision making and finally, reacting by appropriate actions;
- Gathering events in intervals time, comparing them to the predefined thresholds and assigning a state label to them such as notification, warning or normal;
- In this approach, each cluster-head can operate only by using accessible local information on the cluster-wide level; in other words, it can make decision about intrusion occurrence of its cluster nodes, autonomously; of course, it also using a distributed design for decision making on intrusion detection between sensor nodes, cluster-heads and the central server, provide possibility of using a distributed mechanism to take the final decision about intrusion threat.
- In homogenous WSNs, CIDSs are same exactly on entire cluster-heads or sensor nodes and other WSN's components; they can broadcast, eavesdrop and listen to the messages (for example, messages that come from other cluster-heads).
- In heterogeneous WSNs, CIDSs are different than each others and other WSN's components (since the hosting systems and data types are different).
- The main properties of CIDS are:
  - Using local information for intrusion detection (localize auditing);
  - Low error rates (due to existing comprehensive Infobases);

Each cluster-head in the WSN should has been a CIDS by following functionalities (according to the **Figure 7**):

- Cluster-based monitoring: each cluster-head monitors its immediate neighboring and nearby nodes (members of its associated cluster) to gather auditing data;
- Decision making: cluster-head using audit data that gathered on previous stage, to make decision on intrusion threat level based on node, based on cluster and appropriate responses; if necessary, it shares its findings with other neighboring cluster-heads to take proper decision, in collective.
- Reaction: each sensor node and cluster-head has responding mechanisms which allow it to react to the intrusion situations.

Internal components and modules which are existing into the CIDS's architecture are (as shown in **Figure 7**):

- Cooperative and local monitoring: gathering, auditing and filtering primary data for detection engine module; audit data of a CIDS is communication activities into its radio range; these data usually are gathering by listening to the transmissions of corresponding cluster nodes and neighboring cluster-heads (CIDSs);
- Independent and local detection engine (cluster-head level): analyzing and comparing audit data, in attending and considering to the properties, given limitations and predefined rules and enforcing detection techniques; this component stores, imposes and operates rely on specification-based detection method which describes correct operations;
- Collective detection engine: collector and the majority rule enforcement; if there was a document rely on intrusion; this module broadcast the information of local detection process state to the neighboring nodes. The same module in any cluster-head is gathering this information from entire neighboring cluster-heads and enforcing the majority rule to concluding if an intrusion is occurred or not (for taking requirement decisions on boundary nodes).
- Decision making module: including local decision making and cooperative decision making;
- Response module: it is possible to divide responses into two categories, according to the attack nature; *i.e.*: direct response and indirect response; once an intrusion occurred, node or compromised area will be detected and this module will does proper actions; including: disconnecting session, isolating intruder and malicious area (compromised nodes), preventing the malicious/suspicious node from entire WSN's routes, network recovery, improving the used routing protocol, producing and using new secret keys, notifying to the WSNIDS and associated node by corresponding cluster-head (s), reducing the quality estimation of the link to that node. According to the independent and autonomous behavior of WSNs, these functions must be doing without human agent intervention and in limited time.

Communication mechanism: this module is using to establish communication between inter-cluster sensor nodes, neighboring cluster-heads and the central server.

5.3. Wireless Sensor Network-Based Intrusion Detection System (WSNIDS: WSN Wide Level IDS)

The WSNIDS place on the highest level of the proposed architecture; *i.e.* it installs and deploys on the heterogene-

ous central server and management part. As **Figure 8** shows, this is a comprehensive IDS which has some of complete info-bases including a series of comprehensive and integrated policy-bases along with some agents to distinguishing anomalies. Also, the hosting system and deployment location of this IDS is a powerful system which has high software and hardware equipments and capabilities.

Figure 8 represents the basic architecture of the WSNIDS in form of existent main modules and procedures into the system (WSNIDS); this system is doing many activities, such as: distinguishing the referral traffic from cluster-heads, full processing, analyzing and detecting, logging, performing associated and appropriate responses, and then, tracking and forensic analysis (according to **Figures 8 and 9**).

Following figure (**Figure 10**) is showing the data flow into the WSNIDS, in more detailed.

As shown **Figures 8-10**, the WSNIDS is based on analyzing audit data, detected events by cluster-heads and inference the WSN's behaviors. The taken approach in the WSNIDS has following features:

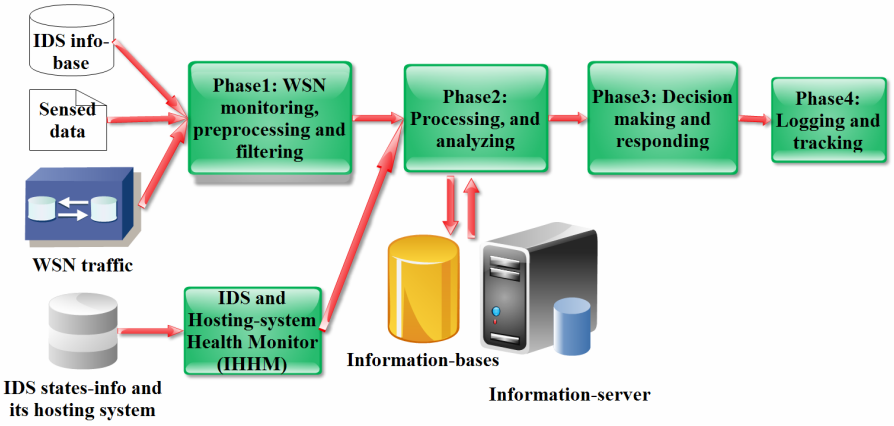


Figure 8. The basis architecture of the WSNIDS.

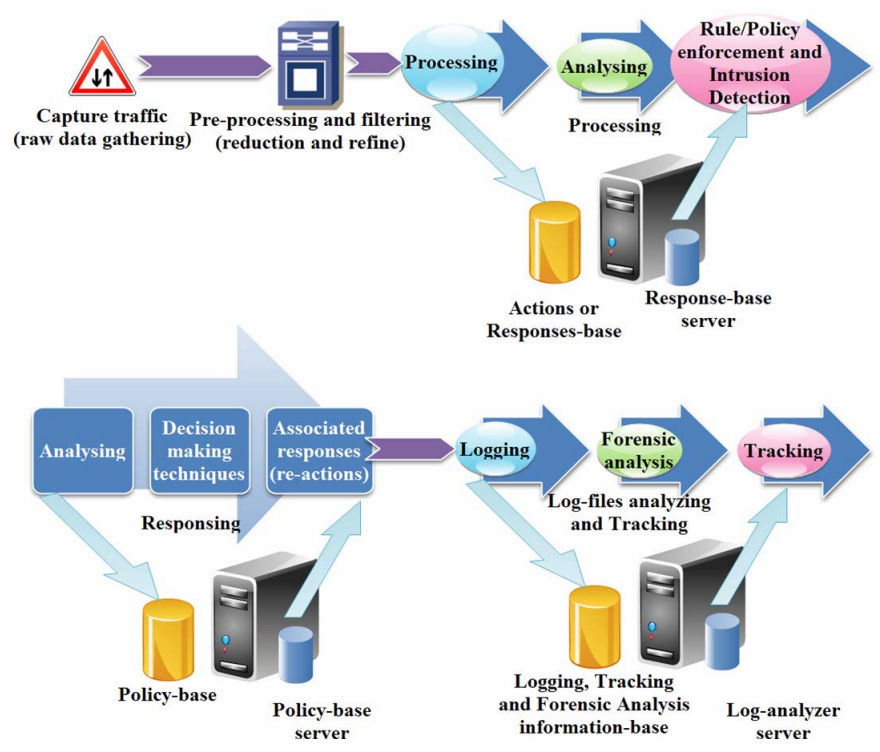


Figure 9. The WSNIDS work flow.

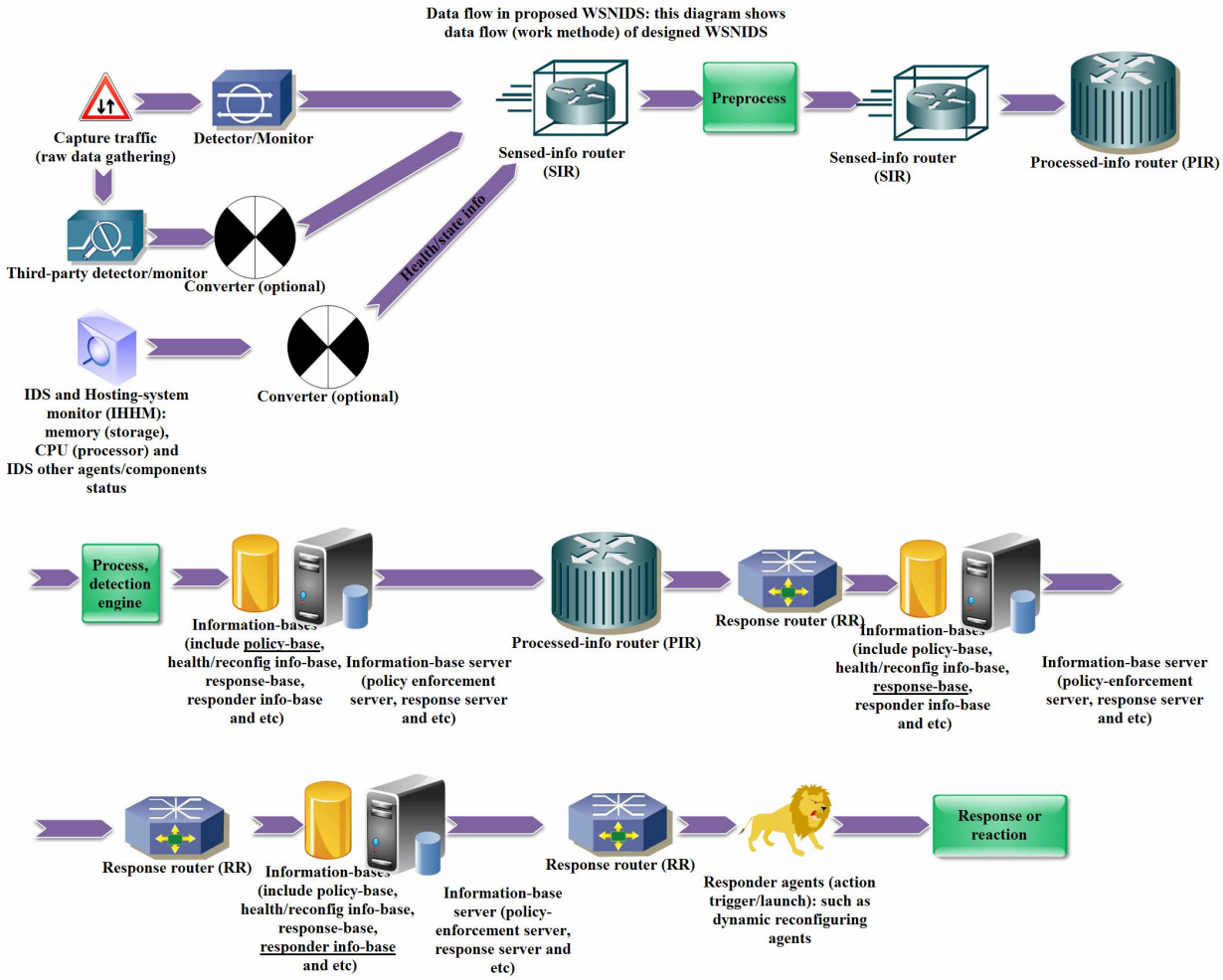


Figure 10. The WSNIDS data flow.

- Using an agent and policy-based platform;

There are four different layers, including: acquisition and preprocessing traffic layer, processing and analyzing layer, decision making and response layer and tracking and forensic analysis layer; also, it has a user interface in different layers.

5.4. The Major Properties of the Proposed Architecture

The suggested system has following features:

- Distributed, hierarchical and cooperation-based structure (based on participation of sensor nodes, cluster-heads and the central system to each others);
- Efficiency, high performance, optimal energy consumption and increase the WSN lifetime and its stability;
- Independent and autonomous SIDSs;
- Independence and autonomous CIDSs; they do not have any dependency to each other, or they have minimum dependency (else about decision making on boundary sensor nodes); however, each CIDS does its functions independently, almost entirely. Most of times, it also takes decisions, itself/alone (else about boundary nodes).
- Ease of extensibility, too much scalability and high flexibility;
- Powerful detection process (since there are SIDSs on sensor nodes, CIDSs on the cluster-heads, WSNIDS on the central server, appropriate policies and rules and comprehensive info-bases);
- IDSs based on agent and policy;
- It allows to use authentication and authorization mechanisms for different levels of the proposed architecture; for example, SIDSs to the associated CIDSs and CIDSs to the WSNIDS, to establishing secure communications between different existent IDSs and preventing from intrusion of unauthorized systems;
- Providing information to tracking attackers (supporting forensic analysis, detecting and finding attackers

on cyber space for preventing from electronic crimes);
- The performance of the proposed model is depending on response time (time consumed to search and finding appropriate pattern for query matching into the info-bases like policy-base);
- Fault tolerant and dynamic reconfiguration:
  - Using backup network equipments, such as sensor nodes in low level and cluster-heads in medium level of the proposed architecture; *i.e.* there are some backup sensor nodes and backup cluster-heads;
  - Using backup agents into the IDSs;
  - Clusters overlapping (increased stability);
  - Existing dynamic reconfiguration agents for each SIDS, CIDS, and the WSNIDS;
  - Updating resources and info-bases in manual or automatic; for example, by using new patterns of attacks, or dynamic and manual/automatic change of thresholds, but in attending to the current conditions of the WSN; or changing the response type once an event occurred;
- Security considerations:
  - IDS protection (monitoring the health state of IDSs and their hosting systems, continuously);
  - The architecture is dependence to the network data flow;
  - Existence logging capabilities;
  - Using cryptography and secret key to exchange information between sensor nodes and associated cluster-heads, and between cluster-heads and the central server (WSNIDS), to preventing from intrusion and avoiding from establishing unauthorized direct communication to IDSs through unauthorized systems.

6. Results

This paper has been designed a questionnaire to verify the proposed system. The prepared questionnaire is including some questions about different aspects and properties of the IDA; it also discusses the high-level and general requirements of IDSs, which focused on IDSs' performance and functionality. The properties and their associated questions are classified into 6 categories, including: processing and managing properties, operational, output, technical and finally, special and high-level properties. The questionnaire is presented to some experts in WSN and IDS areas (almost 50 people). Then, the acquired result has been analyzed and evaluated in form of following tables and figure.

6.1. Preprocessing and Processing Properties

As **Table 1** is showing, the proposed architecture supports different dimensions of IDSs' processing properties. For example, the IDA's monitoring level is almost 98.7 percent; *i.e.* it covers the WSN's components such as sensor nodes, cluster-heads and the central server, almost completely. Also, the extendibility capability of the IDA is about 84.9 percent. Besides, the IDA has dynamic re-configurability capability about 75.6 percent. The suggested system is supporting local/remote control and distributed databases capabilities. It is evaluated the IDA is including the properties of processing and managing category of IDSs' requirements about 86.4 percent, in average.

6.2. Operational Properties

Table 2 is representing the different aspects of the IDA's operational requirements. According to the following table, the IDA supports real-time detection property almost 82.3 percent. Also, it has the content-based (body of a packet) detection and context-based (header of a packet) detection capabilities about 94.5 and 66.8 percent, in order. The proposed system is independent of used platform and Operating System (OS); in other words, it is supporting multiple platforms and multiple OS. The suggested system supports hierarchical reporting structure and it reacts to the attacks, automatically; *i.e.* into the IDA, sensor nodes report and communicate to the cluster-heads and cluster-heads report and communicate to the central server. Finally, the IDA is included the properties of this IDSs' requirement category about 81.2 percent, in total.

Table 1. Processing properties of the IDA.

No.	Question	Functional properties		Non-Functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Monitoring level	—		98.7
2	Extendibility and flexibility	—		84.9
3	Dynamic re-configurability capability	—		75.6
4	Local and remote control capabilities	Yes		—
5	Distributed databases capabilities	Yes		—
	Average (percentage)	—		**86.4**

Table 2. Operational properties of the IDA.

No.	Question	Functional properties		Non-Functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Gathering intrusion detection and vulnerability data in real-time and non real-time	—		82.3
2	Content-based detection capability	—		94.5
3	Context-based detection capability	—		66.8
4	Supporting multiple platforms and multiple OS	Yes		—
5	Hierarchical reporting structure	Yes		—
6	Automatic reaction to the intrusions	Yes		—
	Average (percentage)	—		**81.2**

6.3. Output Requirements

Following table (**Table 3**) shows the IDA has different characteristics in output requirement area, including: it can make attackers profile, security profile and system profile; of course, by attending and using the logged information and data flow into the WSN.

6.4. Technical Requirements

Table4 is representing and questioning the IDA's technical properties. For example, ease of implementation of the proposed system is evaluated about 91.2 percent; the IDA has fault tolerant, scalability, robustness and safety capabilities, each one almost 83.4, 95.1, 72.5 and 78.6 percent, in order. Also, the suggested system can using cryptography and digital signature, key management, authentication and authorization mechanisms to establishing secure connections between different levels of the WSN's components. Besides, the IDA is an efficient system; since it does not enforce extra load to the WSN resources and its normal functionalities. As a result, the proposed architecture supports different properties of this IDSs' requirement category about 84.2 percent, in average.

6.5. Special and High-Level Properties of the IDA

Following table (**Table 5**) represents and considers the required especial and high-level properties of the IDA. As the acquired result of the questionnaires shows, the proposed system has distributed and hierarchical architecture, based on cooperation of sensor nodes, cluster-heads and the central server to each others; also, the CIDSs are independent than each others (about 84.5 percent). The IDA is included centralized management on the WSN resources (such as info-bases) and its components. The proposed system supports localize auditing capability; *i.e.* SIDSs and CIDSs can operate by using partial and local auditing data, in sensor-level and cluster-head level (almost 94.7 percent). This system is included minimize resources property; *i.e.* It has attention to the minimize resources property, in the design phase and it tries to consume energy, in appropriate (90.3 percent). This architecture supports accurate management of resources, non-enforcing extra load to the WSN and monitoring the health state of IDSs and the WSN components. The IDA is including truly distributed property; *i.e.* it is gathering and analyzing data in some determined locations, such as cluster-heads; also, it does not enforce extra load to the some determined nodes (it is using distributed approach about 82.2 percent). The proposed system is a secure architecture; *i.e.* it is resistant and robust against attacks (almost 79.8 percent); so, if one or more sensor node (their SIDSs) or a cluster-head and associated CIDS be compromised, it should not be leads to missing the control on the WSN; for example, removing an authorized node from the network or non-detection of an attacker node. The IDA has centralized control on inter-components data communications and interactions from the central server, by user. The level of interaction between different network components in its different levels to each others in the same or different levels of the network (between sensor nodes and CIDSs, between CIDSs to each others, between CIDSs and the WSNIDS) is almost 93.5 percent. This system can detect chaining attacks by using powerful detection process and audit trial mechanisms (about 65.8 percent). The IDA is evaluated as an optimal system in energy consumption; since, it is attending to the energy consumption in designing step (almost 81.4 percent). The strength of detection process on the proposed system is evaluated about 96.9 percent (because there is strong and big info-bases and hierarchical detection process). The IDA has attention to taking back-up designs; *i.e.* it supports the back-up components and performs operations such as buffering. The IDA's efficiency and its functionality are depending on to the network data flow; its dependability is evaluated almost 86.5 percent. The suggested architecture is consistent to the centralized and autonomous operations in different levels of WSNs; its consistency is evaluated about 89.3 percent. The proposed system is providing the possibility of updating and configuring network components from different control locations; *i.e.* it is possible to configure sensor nodes

Table 3. Output properties of the IDA.

No.	Question	Functional properties		Non-Functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Making attackers profile	Yes		—
2	Providing security profile	Yes		—
3	representing the system profile	Yes		—
	Average (percentage)	—		—

Table 4. Technical properties of the IDA.

No.	Question	Functional properties		Non-Functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Ease of implementation	—		91.2
2	Fault tolerant capability	—		83.4
3	Scalability	—		95.1
4	Robustness	—		72.5
5	Safety (against unauthorized access)	—		78.6
6	Possibility of using key management and authentication mechanisms	Yes		—
7	Enforcing extra load to the WSN	No		—
	Average (percentage)	—		**84.2**

Table 5. Special and high-level properties of the IDA.

No.	Question	Functional properties		Non-Functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Distributed and hierarchical architecture, based on cooperation	Yes		—
2	Undependability of CIDSs	—		84.5
3	Centralized management on the WSN	Yes		—
4	Localize auditing capability	—		94.7
5	Minimize resources property	—		90.3
6	Accurate management of resources and monitoring the health state of IDSs and the WSN components	Yes		—
7	Truly distributed	—		82.2
8	The IDA security	—		79.8
9	Centralized control on inter-components data communications	Yes		—
10	Interaction level between different network components	—		93.5
11	Ability to detecting chaining attacks	—		65.8
12	Attending to the energy consumption	—		81.4
13	Strength of detection process	—		96.9
14	Possibility to taking back-up designs	Yes		—
15	Data flow dependability	—		86.5
16	Consistency to the centralized and autonomous operations of the WSN	—		89.3
17	Existing different control locations	Yes		—
18	Ease of updating	—		84.9
19	Possibility to updating the IDSs (SIDSs, CIDSs and the WSNIDS)and operational using of them, simultaneously	Yes		—
20	Combinational decision making technique	Yes		—
	Average (percentage)			**85.8**

from cluster-heads and the central server; or configuring cluster-heads from the central server. Ease of updating and integrating new capabilities and new functionalities to the proposed system is almost 84.9 percent. It is also possible to update the IDSs (SIDSs, CIDSs and the WSNIDS) and operational using of them, simultaneously. The proposed system supports combinational decision making technique; *i.e.* it is possible to making decisions autonomously (by SIDSs and CIDSs) and if necessary, taking cooperative decisions (by CIDSs, collector and the WSNIDS). As a result, the IDA is included different properties of this IDSs' requirement category almost 85.8 percent, in total.

7. Conclusions

The purpose of this paper is discussing the intrusion detection problem on WSNs and designing an Intrusion Detection Architecture (IDA) for these networks, of course by attending to their constraints. The suggested

system depends on situations, the WSN's application area, the requirement security level and other things such as its cost, can be used and implemented in 1, 2 or 3 levels; including: SIDSs (monitoring the local host) on the sensor nodes, CIDSs (surveillance, monitoring and control in cluster-level) on cluster-heads and the WSNIDS (monitoring and control in the WSN-wide level) on the central management system. The main attributions of the suggested architecture are as following:

- The IDA properties: hierarchical, distributed, scalable fault tolerant, robustness and clustering;
  - Distributed systems are more scalable and more robust;
- The proposed IDSs (SIDS, CIDS and WSNIDS) properties: based on agent and policy, independent and autonomous agents, strong and comprehensive info-bases, dynamically reconfigurable, scalable, component-based and modular, fault tolerant and robustness, high-flexibility, host-based (SIDS) and network-based (CIDS and WSNIDS) architectures;
- Detection method:
  - Combinational (specification-based);
  - Uncentralized (detection in 1, 2 or 3 levels); because these networks are application-oriented;
- Decision making approach: combinational;
  - About each sensor node, the associated SIDS makes decision, independent and autonomously;
  - About each cluster, the corresponding cluster-head (CIDS) makes decision, independently and autonomously;
  - About anomaly occurrence or boundary nodes, associated SIDSs and CIDSs, collector and the WSNIDS make final decision, cooperatively;
  - About some cases of anomalies, existent information is presented to the human agent;
- Response method: combinational; *i.e.* active response and passive response, depending on to the conditions and the attack's nature;
- Fast and real-time detection process and response: reducing the response time by using caching and buffering techniques to preventing from scrolling the entire file for a repeated event or using better mechanisms for query in policy-bases; besides, SIDSs and CIDSs are very near to attackers;
- Comparative and multi-agent detection process to detecting attacks along with low error rate;
- The heterogeneous WSN and IDSs;
- Consistent with automatic, autonomous and independent mechanisms of WSNs;
- Possibility of centralized management on systems and resources by using the WSNIDS;
- Focused on routing layer, mainly;
- According to the **Tables 1, 2**, **4 and 5**, the following table (**Table 6**) is representing integrated average values of different IDSs' requirement classes.
- According to the **Table 6**, following figure (**Figure 11**) is formed. **Figure 1** is showing the sum average values of different IDSs' properties categories; in other words, the IDA supports different categories of IDSs' required properties (as **Figure 11** shows).
- As above figure shows, the processing and managing properties of the suggested system has been assessed almost 86.4 percent, in average; *i.e.* the IDA supports different aspects of this requirement category about 86.4 percent. Also, the supported operational and technical properties by the proposed architecture have been evaluated about 81.2 and 84.2 percent, in order. The proposed system is included especial and high-level required properties of IDSs almost 85.8 percent, in general. As a result, the proposed system is included different IDSs' requirement categories almost 84.3 percent, in total average.

In summarize, the posed model in this paper is a comprehensive model which has some main properties such as robustness, scalability, responsively, extensibility and incremental matching along with environment changes and its new conditions. Also, the IDA is focused on integrating the accessible tools in security area of computer networks (like IDSs, logging, tracking and forensic analysis systems). This model is a distributed model for intrusion detection on WSNs, which it is designed as even it can operates by only using minor and local accessible information in each sensor node, cluster and cluster-head; *i.e.* it can uses from the local sensor-level and cluster-wide information to detects intrusions by SIDSs or CIDSs. Also, if necessary, sensor nodes, cluster-heads and the central server cooperate to each others to take an appropriate decisions about if an attack occurred, or not; in other words, they share their information to each others, with associated CIDSs, collector and if necessary, with the WSNIDS, to detect and make final decision on detected anomaly. It is hoped to this research able us to

Table 6. Total average value of different properties category.

No.	Properties class	Total average value (in percentage)
1	Preprocessing, processing, assessing and managing properties	86.4
2	Operational properties	81.2
3	Technical properties	84.2
4	Special and high-level properties	85.8
	Average value (in percentage)	**84.3**

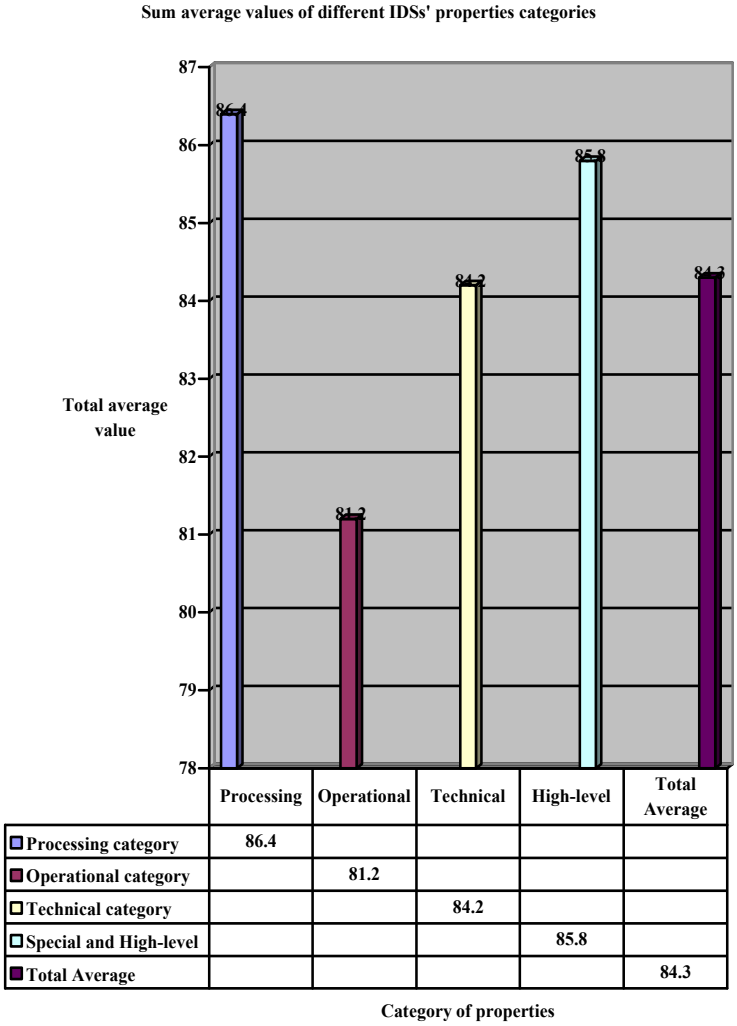


Figure 11. The sum average values of different IDSs' properties categories.

improving the security level of WSNs.

8. Future Works

Some of research areas in this domain to improve and extend the proposed model capabilities are:

- Improving response scheduling, priority responses and having more control on response production mechanism;
- Providing higher level of security, fault tolerant and robustness for suggested architecture;
- Centralizing more detailed information about system activities for forensic analysis;
- Efficient data management;
- Developing user friendly interfaces which allow dynamic reconfiguration of systems (the SIDSs, CIDSs and the WSNIDS) and representing the activities of these systems, in graphical;
- Approaches for data aggregation in WSNs' different protocols;
- Techniques for using of mobile nodes in WSNs;

Work in this area always is growing and as the WSNs are changing, and their utility, performance and application are increasing, the security threats also are increasing; so, architectures and IDSs to protecting WSNs against different types of attacks will be required, more and more.

9. References

[1] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," *International Journal of Information Assurance and Security*, Vol. 6, No. 3, 2011, pp. 195-215.

[2] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," *International Journal of Information Security*, Vol. 2, No. 2, 2011, pp. 69-84.

[3] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks," *International Journal of Information Assurance and Security*, Vol. 6, 2011, pp. 331-345.

[4] B. Krishnamachari, D. Estrin and S. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," *International Workshop on Distributed Event-Based Systems*, Vienna, July 2002, pp. 457-458.

[5] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," *International Journal of Computers and Their Applications*, Vol. 1, Special Issue on "Mobile Ad-hoc Networks", 2010, pp. 42-45.

[6] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Physical Attacks on Wireless Sensor Networks," *International Journal of Peer to Peer Networks*, Vol. 2, No. 2, 2011, pp. 24-42. doi:10.5121/ijp2p.2011.2203

[7] M. Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification," Department of Computer Science, Purdue University, 2011. https://www.cerias.purdue.edu/apps/reports_and_papers/view/3106

[8] T. A. Zia, "A Security Framework for Wireless Sensor Networks," Doctor of Philosophy (PhD) Thesis, The School of Information Technologies, University of Sydney, 2008.

[9] A. Perrig, R. Szewczyk, V. Wen, D. Culler and D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Proceedings of 7th Annual International Conference on Mobile Computing and Networks*, Rome, July 2001.

[10] Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks," Department of Electrical and Computer Engineering, University of Waterloo, Canada, 2011. http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-20.pdf

[11] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," *Elsevier's Computer Networks*, Vol. 52, No. 12, 2008, pp. 2292-2330. doi:10.1016/j.comnet.2008.04.002

[12] A. Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN, Department of computer science," *Faculty of Electrical Engineering and Information Technology*, Skopje, 2011. http://ict-act.org/ICTInntions.../ictinnovations2009_submission_21.pdf

[13] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Alaska, 11 May 2003, pp. 113-127.

[14] R. A. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," *Computer Society*, Vol. 35, No. 4, 2002, pp. 27-30. doi:ieeecomputersociety.org/10.1109/MC.2002.10036

[15] Ch. Krügel and Th. Toth, "A Survey on Intrusion Detection Systems," TU Vienna, Austria, 2000.

[16] A. K. Jones and R. S. Sielken, "Computer System Intrusion Detection: A Survey," University of Virginia, 1999.

[17] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST 800-94, Feb 2007.

[18] G. Maselli, L. Deri and S. Suin, "Design and Implementation of an Anomaly Detection System: an Empirical Approach," University of Pisa, Italy, 2002.

[19] S. Northcutt and J. Novak, "Network Intrusion Detection: An Analyst's Handbook," New Riders Publishing, Thousand Oaks, 2002.

[20] V. Chandala, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey, ACM Computing Surveys," University of Minnesota, September 2009.

[21] J. Molina and M. Cukier, "Evaluating Attack Resiliency for Host Intrusion Detection Systems," *Information Assurance and Security Journal*, Vol. 4, 2009. pp. 1-9.

[22] S. Zanero and S. M. Savaresi, "Unsupervised Learning Techniques for an Intrusion Detection System," *Proceedings of ACM Symposium on Applied Computing*, New York, 2004, pp. 412-419. doi:10.1145/967900.967988

[23] S. Selliah, "Mobile Agent-Based Attack Resistant Architecture for Distributed Intrusion Detection System," MSc Thesis, College of Engineering and Mineral Resources at West Virginia University, 2001.

[24] O. Depren, M. Topallar, E. narim and M. K. Ciliz, "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks," *Expert Systems with Applications*, Vol. 29, No. 3, 2005, pp. 713-722.

[25] V. Handziski, A. K'opke, H. Karl, C. Frank and W. Drytkiewicz, "Improving the Energy Efficiency of Directed Diffusion Using Passive Clustering," *Proceedings of 1st European Workshop on Wireless Sensor Networks*, Berlin, 2004, pp. 172-187.

