Int. J. Communications, Network and System Sciences, **2011, 4, 523-543**
doi:10.4236/ijcns.2011.48064 Published Online August 2011 (http://www.SciRP.org/journal/ijcns)

Designing an Agent-Based Intrusion Detection System for Heterogeneous Wireless Sensor Networks: Robust, Fault Tolerant 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 26, 2011; *revised June* 22, 2011; *accepted August* 8, 2011

Abstract

Protecting networks 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 architecture of Intrusion Detection System (IDS). The main contribution of this architecture is its modularity and flexibility; *i.e.* it is designed and applicable, in four steps on intrusion detection process, consistent to the application domain and its required security level. Focus of this paper is on the heterogeneous WSNs and network-based IDS, by designing and deploying the Wireless Sensor Network wide level Intrusion Detection System (WSNIDS) on the base station (sink). Finally, this paper has been designed a questionnaire to verify its idea, by using the acquired results from analyzing the questionnaires.

Keywords: Wireless Sensor Network (WSN), Security, Intrusion Detection System (IDS), Modular, Attack, Process, Detection, Response, Tracking

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" and "sink or base station" (*i.e.* the WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes [1]. 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 [11]. Factors such as wireless, unsafe, unprotected and shared nature of communication channel, un-trusted 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 [2,3]. 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 detects unsafe activities and unauthorized access; also, when attacks occurred, even new attacks such as anomalies, it can notify by different warnings and perform some actions (mainly predefined actions). Therefore, the main purpose of this paper is discussing and solving the intrusion detection problem on WSNs.

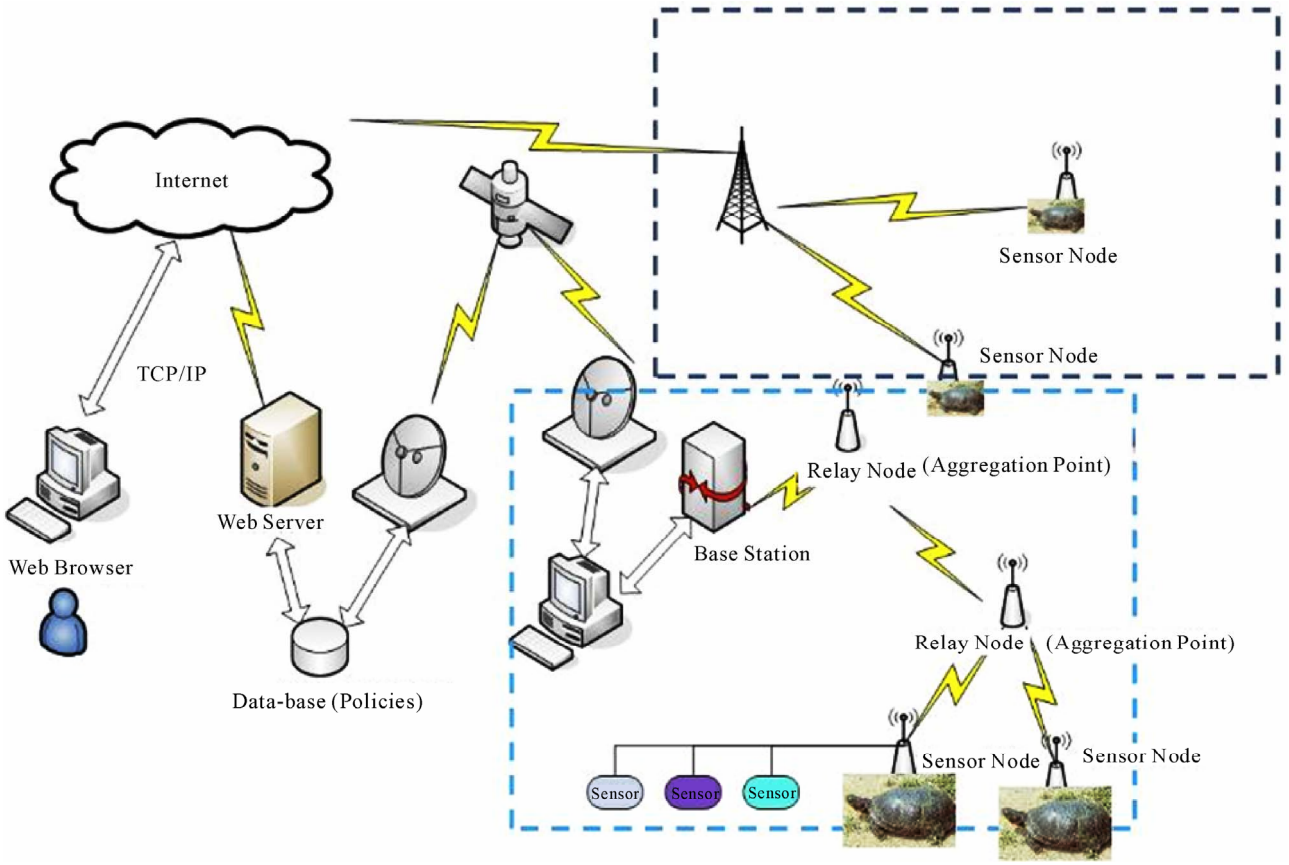


Figure 1. WSNs' communication architecture.

This paper is focused on following topics:

- An overview of WSNs and their security;
- Discussing Intrusion Detection System (IDS) as a new aggressive-defensive security layer for WSNs;
- Suggestion a comprehensive, modular and centralized Intrusion Detection System for WSNs (the WSNIDS).

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' 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's requirements in these networks; Section 5 will describe architecture of the proposed Intrusion Detection System for WSNs (WSNIDS); Section 6 prepares a questionnaire to verifying the proposed system; it also expressed the reached results from analyzing questionnaires; Section 7 is 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 value of physical parameters or an event occurrence; then, it converts that value to electrical signal; finally, if necessary, it actuates to the event by using electrical actuators [1,24]. Major features of WSNs are:

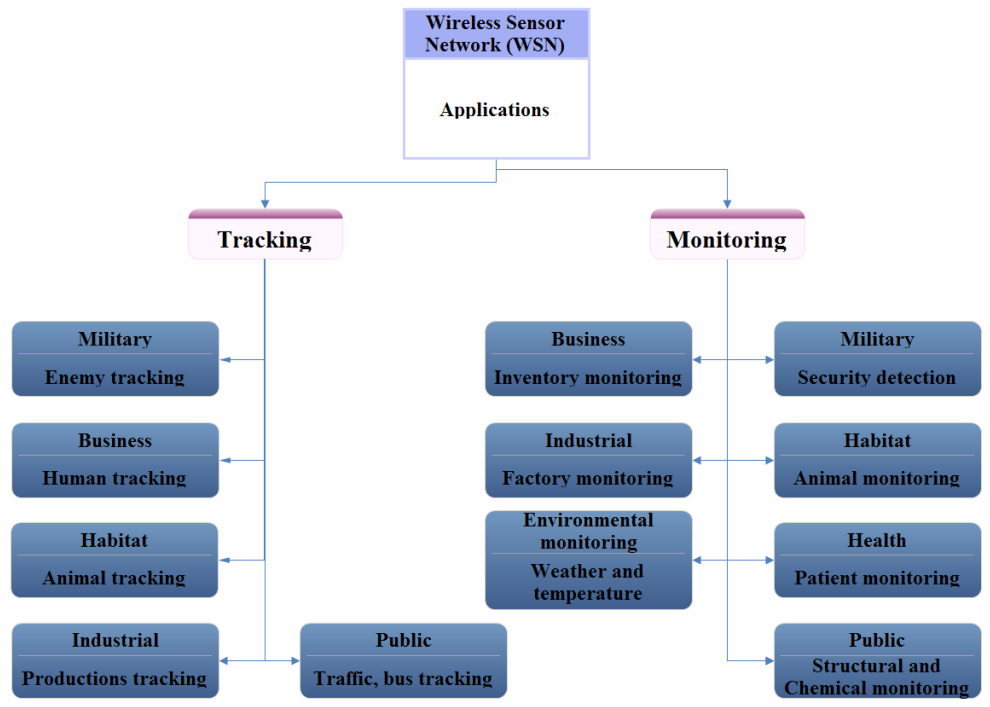
- Infrastructure-less [1,2,25];
- No public address, often (data-centric network) [2,5];
- Consists of many (hundreds or thousands) tiny sensor nodes [4,10] (small size, low-cost and low-power);
- High-density of nodes distribution [6,25];
- Insecure radio links;
- Application-oriented;
- Different communication models [1,2,8], including: hierarchical/distributed WSNs; or homogenous/heterogeneous WSNs;
- Limited resources of sensor nodes [2,3,7] (radio communication, bandwidth, energy, memory and processing capabilities) [5,6,9];
- 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 applications of these networks are: military, medical, environmental monitoring, industrial, infrastructure protection, disaster detection and recovery, agriculture, intelligent buildings, transportation and space discovery (as shown in **Figure 2(b)**).

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

2.1. WSNs Characteristics

A WSN is a homogenous or heterogeneous network consisting of hundreds or thousands tiny sensor nodes to monitor and gather real-time information from operational environment [2,7,24]. Common functionalities sensor nodes are broadcasting and multicasting, routing,



(a)

(b)

Figure 2. WSN's applications.

forwarding and route maintenance. The sensor's components are: sensor unit, processing unit, memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other, as shown in **Figure 3**. Some of most important properties of WSNs are:

- Wireless and weak connections [1,3,8];
- Low reliability of sensor nodes;
- Dynamic topology and self-organization [2,4,24];
- Ad-hoc based networks and hop-by-hop communications (multi-hop routing);
- Hostile nature of operational environment [2,5,9];
- Autonomous sensor nodes (local view and independent decision making capability);
- Cooperation of sensor nodes and other WSNs' components to each others (global view);
- Broadcast-nature of communications between sensor nodes [3,7];
- Ease of extendibility (scalable);
- Direct interaction with physical environment [1,6];
- Single-purpose and application-oriented networks;
- Automatic [10] and non-interrupted operations [6];
- Management the communications between mobile nodes [24];
- Hardware limitations of sensor nodes [1,2,7].

2.2. Different Types of WSNs' Architectures

As shown in following figure (**Figure 4**), on WSNs' architecture, there are components such as sensor nodes (motes that are sensing data), aggregation points, sink [1,2], network manager, security manager, and user interface [8,10]. These components participate to each others to the WSN operates, correctly. **Figure 4** shows different kinds of WSN's architectures; as follows:

2.2.1. Direct Communication Architecture

- Each sensor nodes communicates to the sink, directly [9]. Thus, this architecture is not appropriate for wide WSNs; *i.e.* it is not scalable.

2.2.2. Multi-hop and Peer-to-Peer Architecture

- Sensor nodes have routing capability [8];

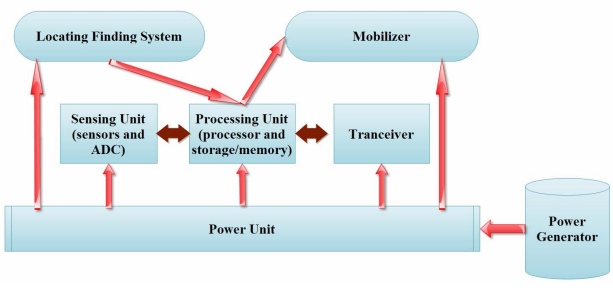


Figure 3. Architecture of sensor node.

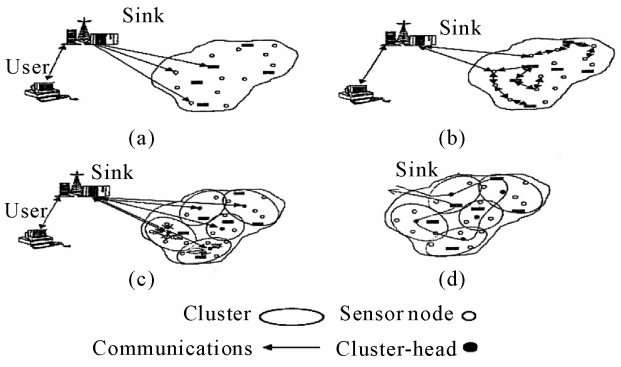


Figure 4. Different types of WSNs' architectures: (a) Direct communication architecture; (b) Multi-hop and peer-to-peer architecture; (c) Multi-hop based on clustering architecture; (d) Multi-hop, clustering and dynamic cluster-heads architecture.

- This architecture is not scalable [10]; because sensor nodes which place nearby to the sink, they are using for packets routing between other nodes and the sink, usually; therefore, if the WSN be widespread, traffic of such nodes will increase; consequently, their energy will be waste, consumed and finished; so they go out of the WSN, in fast.

2.2.3. Multi-hop Based on Clustering Architecture

- Sensor nodes make a clustering structure [9,10];
- Choosing a cluster-head for any cluster [8]; each cluster-head can communicate to the sink, directly; thus, each clusters' nodes send their gathered data to the corresponding cluster-head;
- Problem: most communication operations are doing by cluster-heads; thus, their energy will be consumed, reduced and wasted, sooner than other nodes (if the cluster-heads be had weak capabilities or on homogenous WSNs);
- Solution: changing the role of cluster-head between corresponding cluster nodes, dynamically; or using from strong and heterogeneous cluster-heads.

2.2.4. Multi-hop, Clustering and Dynamic Cluster-Heads Architecture

- This architecture solves the weakness of previous architecture by dynamically change the role of cluster-head among corresponding cluster's nodes.

2.3. Vulnerabilities and Challenges of WSNs

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

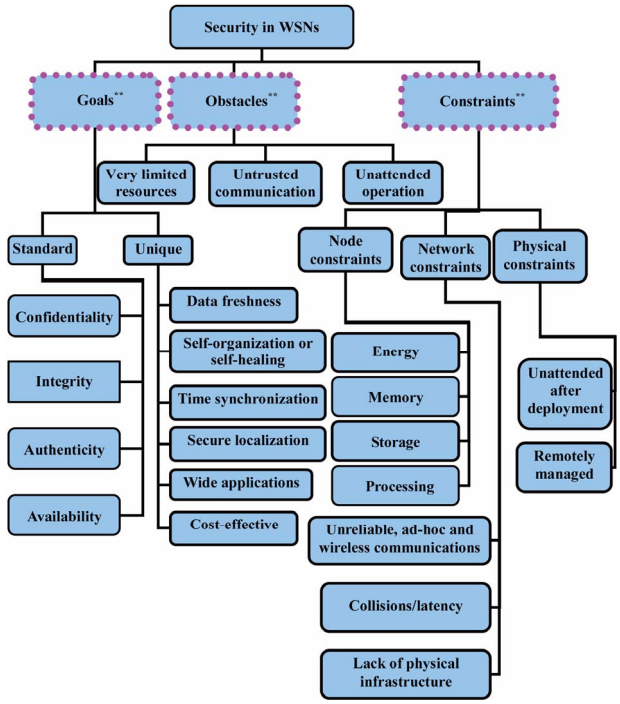
- Theft [1,2] (reengineering and replicating) [3,25];
- Limited capabilities and resources [2,3] (DoS attacks risks, constraint in using encryption);

- Random deployment [5] (hard pre-configuration);
- Deployment on open/dynamic/hostile environments [2,6] (physical access, capture and node destruction);
- Insider attackers;
- Inapplicable traditional network's common security techniques [2,3] (due to limited resources, deploying on open environments and direct interaction to physical environment);
- Requirement to redesigning security architectures and protocols;
- 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 [1,2,25];
- Dynamic topology and self-organization [1,25];
- Sensor nodes' selfishness [2,7];
- Requiring to forwarding and routing sensed information to a shared destination, called sink;
- Existence redundancy in gathered traffic;
- Fault tolerant [1,7];
- Cost of sensor nodes' development and their production [2,24];
- Size and precision of sensor nodes.

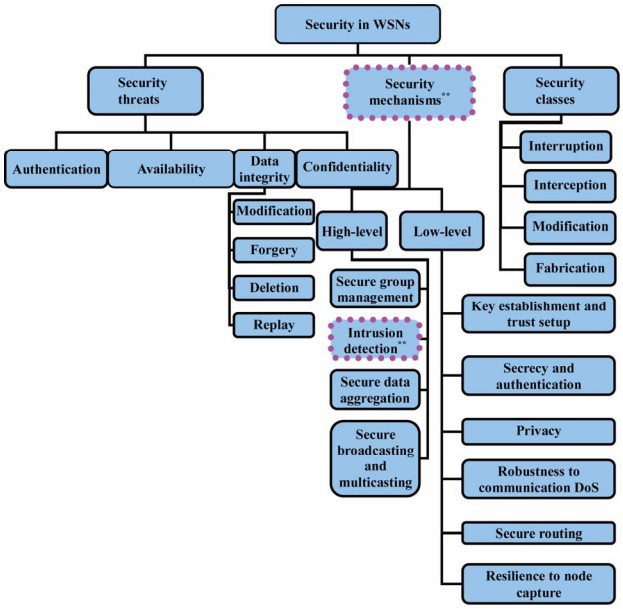
2.4. Security in WSNs

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 [3,8] 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 [2,5];
- Limited resources and un-trusted sensor nodes [1,4];
- Requiring trusted center for key management, to authenticate nodes to each others, preventing from existent attacks and selfishness [1,6,9] and extending collaboration [2];
- Broadcast and wireless nature of transmission media [1,3];
- Sensor nodes deploy on hostile environments [1,7,24] (unsafe physically);
- Unattended nature and operation of WSNs [1,2,10];
- Some of most important dimensions of WSNs have been shown in following figure (**Figures 5(a)** and **(b)**) by star spangled (starry boxes). As **Figure 5(a)** shows,



(a)



(b)

Figure 5. Security in WSNs.

in this paper we have emphasize on goals, obstacles and constraints of WSNs' security aspects. Also, **Figure 5(b)** is showing which this paper has been emphasized on intrusion detection approach from the 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) [23]; 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 [16,19]. Intrusion detection is a process which detecting contradictory activities with security policies to unauthorized access or performance reduction of a system or network [23]; 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 [13,14];
- Usable on host, network [20] 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 [14, 20] (to detecting new attacks and anomalies such as determining thresholds);
- Informing and warning to the security manager [13, 15,19] (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) [13,16] 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 6**, Intrusion Detection Systems (IDSs) attending to the information gathering source and input data supplier, divide into three categories, as follows.

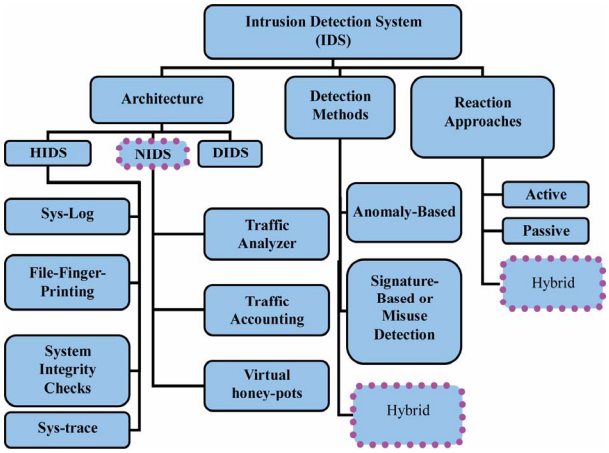


Figure 6. Different categorizations of IDSs.

3.1.1. Host-Based Intrusion Detection System (HIDS)

HIDS installs on a computer system [14,16]; it uses processor and memory of that system and protects only the hosting system [16,17]. It has an abnormal detector part which using statistical methods to detect abnormal behavior of users in comparison to their behavioral records [17,21]; 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.

3.1.2. Network-Based Intrusion Detection System (NIDS)

NIDS is a software process which installs on a special hardware system [15,19]; 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 [14,20,21]. NIDS can identify attacks, on network level; thus, it includes following steps:

- Setting up the Network Interface Card (NIC) on promiscuous mode and eavesdropping network traffic [19];
- Capturing the transmitting network packets [20];
- Extracting requirement information and properties from the network's 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 [18];
- Sending the reports of distributed IDSs (HIDSs and NIDSs) to the central management system;
- Based on distributed and heterogeneous resources [14,

15,18];
- High complexity, variable specifications and agent-ased.

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's traffic as data source; it eavesdrops and listens to the network traffic, captures packets in real-time, then controls and tests them to detect attacks.

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 6** shows, IDSs be partitioned into two categories, based on data analysis and detection method [13,16]. In following sections, they will be considered.

3.2.1. Anomaly Detection Systems

Anomaly Detection Systems are focused on normal behavioral patterns [14,15]. According to the expert systems are not able to timous update patterns, we will need automatic devices to extract new attacks' patterns [15,16, 21]. 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 [13,22]; 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 [15,21] (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 [13, 22]; in this model, IDS gathers the properties of attacks and abnormal behaviors and then, make an information base by them [14,15,21]. 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 [15,16];
- Requiring to a set of predefined patterns [13,22] (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 centralized; because there is the WSNIDS on the sink (highest level of the WSN) and it detects intrusions and makes decision about attack occurrence on the sensor nodes.

3.3. IDS Categorization Based on Response Method

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

3.3.1. Direct 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.

3.3.2. Indirect Response

These kinds of responses do not prevent from the attackers' activities, directly [13,14,16]; like: shunning, logging, notifying [20] through cell phone, email and message to SNMP console [14,15].

⇨ The proposed response approach for the WSNIDS is using combinational method; *i.e.* active and passive responses by each others, depending on conditions and attacks' nature; 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 [5,13]. 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 [10,12]; *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, leads to non-existence unique IDS and requiring different IDSs; so, requiring to a modular and comprehensive IDS [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 install on the sensor nodes and the sink, to saving existent energy consumption; as a result, leading to increase the WSN's lifetime;
- Limited resources [1,5,9,13];
- Unreliable sensor nodes;
- Application-oriented networks [8];
- Requiring to the monitoring, detecting, decision making and responding to the intrusions, in real-time; 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; storage medium; supporting different queries from sensor nodes and the sink; data indexing; 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 [8,12]. 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;
- 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.

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

- Error management, health state monitoring and security management: the WSNIDS can not suppose that any single node is fully secure (supposition: no node is secure); because sensor nodes are compromising easily and disclosure information.
- Accurate and comprehensive monitoring: data gathering and analyzing them at some of specific location (for example, the sink).

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

- Robustness and fault tolerant: the WSNIDS must be robust and resistant against attacks [13,15]. Compromising one or more sensor node and controlling them or compromising the WSNIDS, should not able attackers to remove an authorized node from the WSN or prevent from detecting 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) data communications and interactions;
- Scalability;
- Reaction and tracking capabilities;
- Ease of use (such as standard interfaces);

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 [14, 16]; 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; 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; 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 centralized; *i.e.* there is a comprehensive IDS on highest level of the WSN's architecture which it be installed and deployed on the powerful sink, calling the WSNIDS. It makes decision about occurred intrusions on the sensor nodes, autonomously and independently.

5. Architecture of the Proposed Intrusion Detection System for WSNs: WSNIDS (Wireless Sensor Network Wide Level Intrusion Detection System)

The WSNIDS place on the highest level of the WSN's architecture; *i.e.* it installs and deploys on the heterogeneous sink and management part. As **Figure 7** 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 attacks and anomalies. Also, the hosting system and deployment location of the WSNIDS is a powerful system which has high software and hardware capabilities.

In this section, we would like to discuss about required agents in designing IDS for WSNs and their properties. In the proposed architecture, it is possible to classify agents into four categories; which each phase have some of independent agent (according to the **Figure 7**). Each agent is a set of functionality and internal capabilities of a logical processing unit; also, it is a component of IDS that participate into the intrusion detection process; including:
- Phase 1: monitoring, collecting raw data and preprocessing mechanisms (auditing and filtering);
  - Filtering: filters are software modules that process, aggregate and store incoming data to the IDS. Extracting data from the packets and store into a data-base.
  - Capture traffic and preprocessing: in this step, the messages are eavesdropped and gathered; then important information[1] be filtered and stored for next analyzing.
- Phase 2: processing, analyzing, rule-enforcement and intrusion detection: in this step, the existent rules into the policy-bases are imposed to the stored data. Each input according to a trial of special rules for any type of message, have been assessed: if a message matched and detected as a malicious message, the failure counter increases one. Now, that message has been dropped and no another rule will be enforced it; because the WSNs have severe limited resources. This strategy is reducing the detection latency, too (there is trade off between accuracy, processing cost and run time). Rules are enforcing to the stored data, in order of their complexity. After the message is controlled per all of rules and it not be matched by no one, that message be accepted (once the first match occurred, another rules do not consider, due to savings resources such as power, energy and time);
- Phase 3: decision making and responding techniques;
- Phase 4: logging, tracking and forensic analysis.

Figure 7 represents the basic architecture of the WSNIDS in form of existent main modules and procedures into the system (WSNIDS); this system is performing many activities, such as: distinguishing the referral traffic from sensor nodes, full processing, analyzing and detecting, logging, performing associated and appropriate responses, tracking and forensic analysis (according to the **Figure 7** and **Figure 8**).

5.1. Agents of First Phase of Intrusion Detection Process

The purpose of this phase is monitoring, gathering, pre-

[1]Including fields of packets that can be used in rule-enforcement phase; thus, it leads to the less consumption/waste of the memory and less processing time; then, leads to energy consumption.

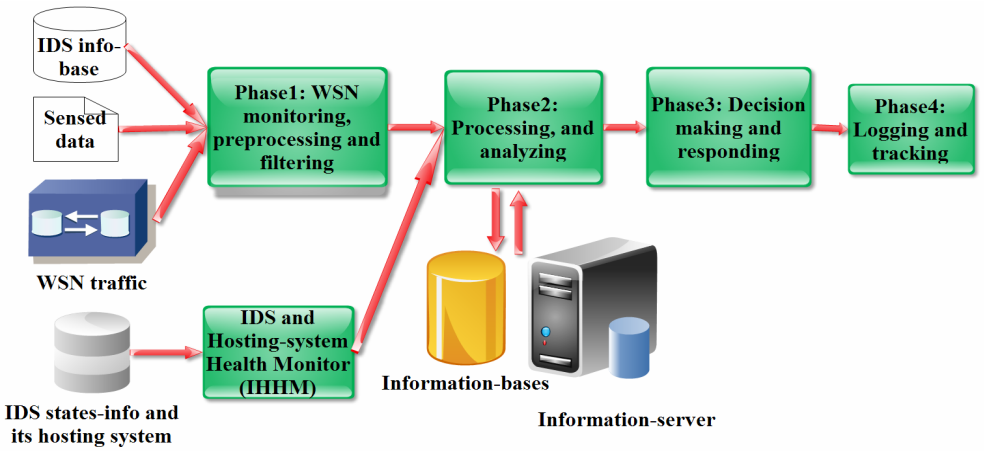


Figure 7. The basis architecture of the WSNIDS (intrusion detection process in the WSNIDS).

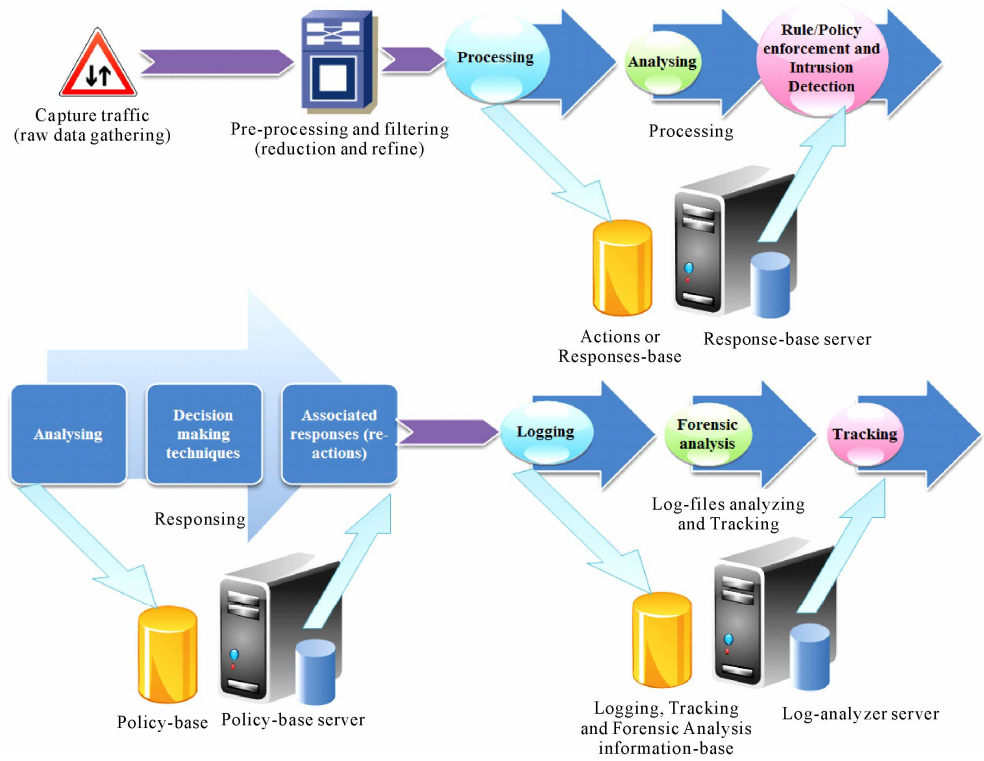


Figure 8. The WSNIDS work flow.

processing and centralized management of data. This package collects and analyzes the intrusion detection data. Thus, the first phase means primary analysis and detection attack or anomaly (parsing, reduction and refining gathered data; then, produce and send events through sensed-info router to next step). In attending to the **Figure 9**, the existent agents into this phase are:

- Detector: data collection; this agent depending on to the application domain and special properties of the WSN, monitors and logs especial events.
  - Using as data pre-processor, processor and filter (data reduction and refining);
  - There are different types of detectors into the WSNIDS, due to listen and eavesdropping different types of data;
  - Detectors are intelligent analyzers which collecting important information about host and network and they are producing events for analyzing, processing and responding. They are at the lowest level of the proposed system, but they are ears and eyes of the WSNIDS;
  - The complexity of this agent is based on its design

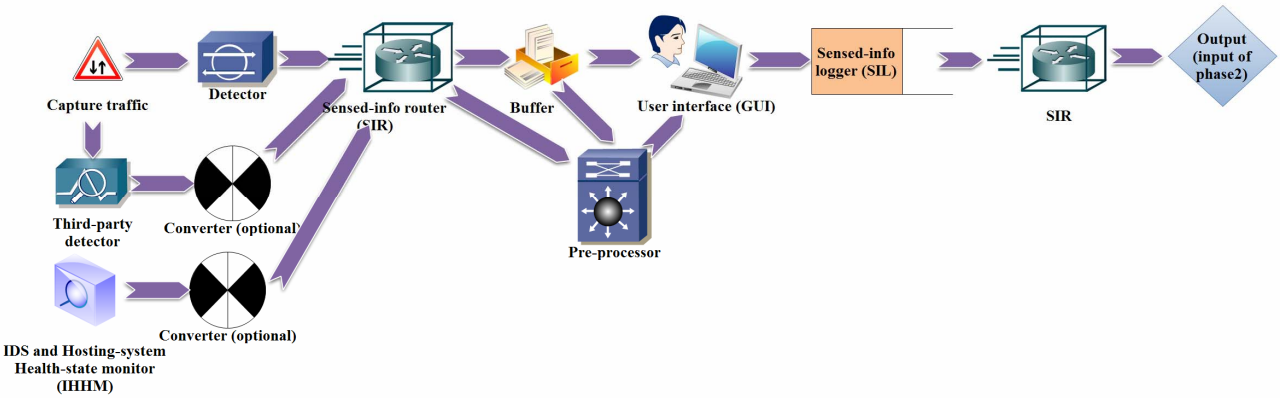


Figure 9. The first phase of intrusion detection process by WSNIDS: data gathering and preprocessing.

and independent from the proposed architecture; detectors are independent agents for monitoring and presenting standard reports like according to the ECA (Event or Sensed-data, Conditions, Actions or Responses) model format;

- Detector is a package consist of some different modules to monitoring ports, log files and existent information into the WSNIDS; also, there are different types of detectors in attention to the operational environment and data types which should be gathered (such as pressure, temperature, speed). Some of its components are: reduction and refiner;

- Converter: format converter interface; by using this module, it is possible to almost integrate each detector to this system.
  - Using of third-party detectors (converting the data to the format of the WSNIDS);
  - It is possible to integrate converter with detector; but it is better that they be as two independent and isolated components;
  - This module produces events which they are input of next step; *i.e.* they send for processing;
  - Using as controller (trigger/stop/reconfiguration detectors).
- Graphical user interfaces (GUI).
  - Displaying reports and graphs to the user.
- IDS and Hosting-system Health Monitor (IHHM): monitoring the health states and systemic parameters (such as CPU usage, Disk utilization, Virtual memory and active processes) of the WSNIDS and its hosting system, periodically; since making sure from the stability of the network and host has special importance. The performance of the WSNIDS is depending on to the state of its hosting system. So it is required a dedicated agent to monitoring the activities of the host. This module evaluates the health-state of the hosting system and information in always and depends on to the state of that system, create the system's health information; then, it analyzes the risk of malicious activity and system state and in attending to it, it presents and proposed some of pre-defined actions.
- Sensed-info-logger (SIL): logging all of input data.
  - Logging controller: controlling such as the volume/size of logged data.
- Sensed-Info Router (SIR): a module which listen to one or many ports; it is always alive state; SIR into the monitoring and preprocessing process operates and participates as a router and logging components (routing, logging routed/malicious/preprocessed events and agents' states); besides, if necessary, it activates other agents (if they be inactivated).
  - Fault tolerant IDS: SIR is a process that receives events from whole detectors, verified them and then, routed them to their destination. So, events that come from detectors and converters are categorized into two classifications; logging requirements and reporting anomalies; SIR is ablating to take deterministic actions, independent from other components; so, it allows to the WSNIDS that be fault tolerant;
  - Another important attribution of the SIR is agent authorization which this attributes blocks the events that try to establish a connection to it.
- Buffer and its controller.

5.2. Agents of Second Phase of Intrusion Detection Process

The second phase is included agents for detection based on agent and policy; this phase produce events that be used as input data of next step; *i.e.* decision making and responding. According to the **Figure 10**, the existent agents into this phase are:

- Detection Engine (DE) module,
  - analyzer and parser;

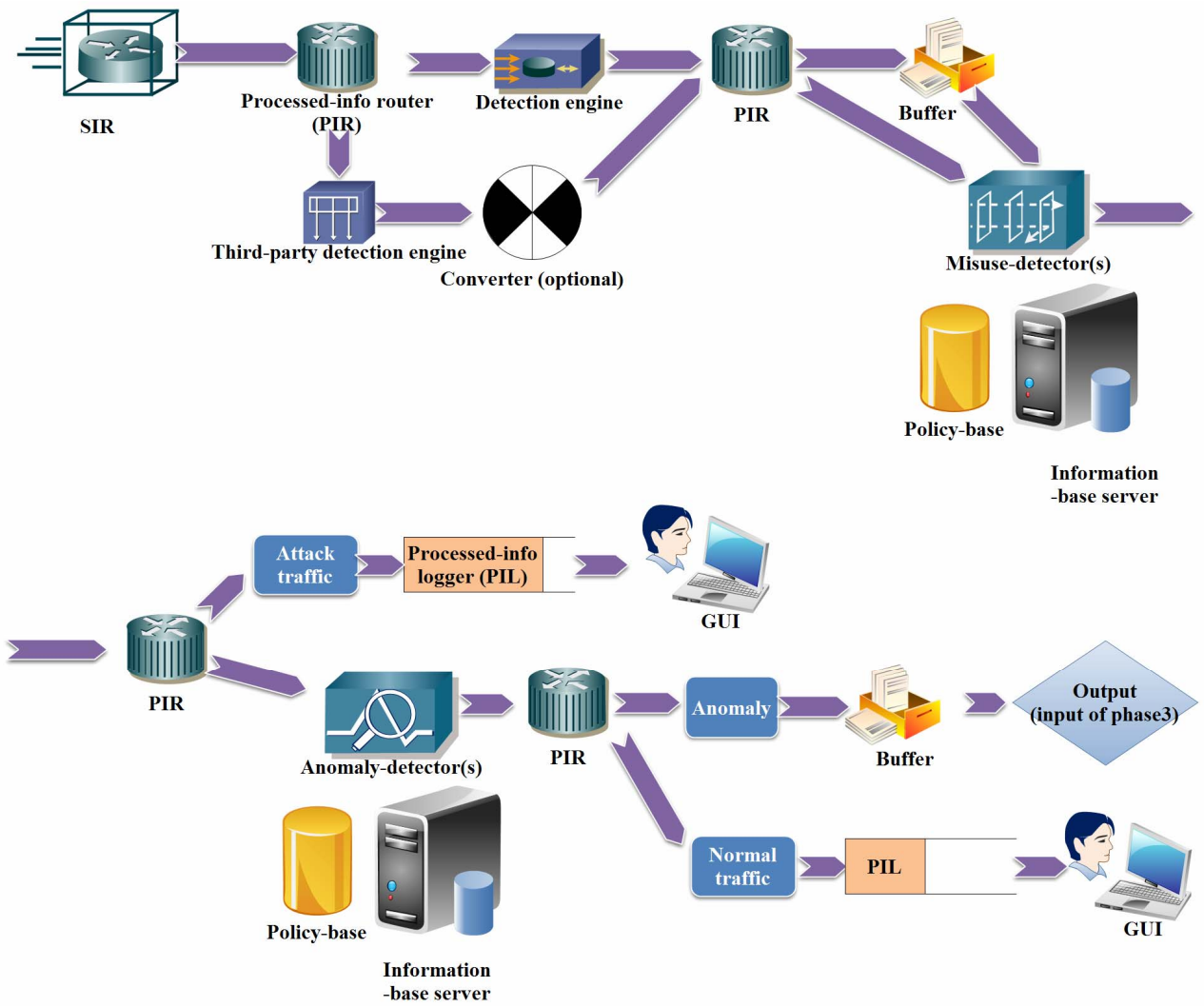


Figure 10. The second phase of intrusion detection process by WSNIDS: analyzing and intrusion detection.

- processor and matcher;
- Audit trial agent (ATA).

- Converter: intermediate of format conversion; this module provides integrating possible of almost any third-party detection engine (TPDE) with the WSNIDS.
  - It is possible to merge converter with detection engine; but it is better that they be separated from each other and be as two independent and isolated modules;
  - Role playing as data processing (reducing the received data to next step);
  - Role playing as controller (trigger/stop/reconfiguration of third-party detection engine).
- Graphical user interfaces (GUI).
  - Displaying reports and graphs to the user.
- Processed-info logger (PIL): logging the whole of processed data.
- Logging controller.
- Processed-Info Router (PIR): routing the processed information (to sending them to the next steps and other agents into the current phase); always alive state; this module cooperate in detection process as a router and logging devices (logging and routing of routed events, agents' states, malicious events and processed events); besides routing, if necessary, it activates other agents (if they be inactivate).
  - Fault tolerant IDS: PIR is a process which receives events from all of detection engines, verified them and then, route them to their destination (next step and other agents of current phase). So the received events are into two categories: internal events (that come from the current step components) and external events (they come from detectors and converters; they are including two types: logging requirements and reporting anoma-

lies). PIR able to take deterministic actions, independent from other agents; thus, it allows to the WSNIDS that be fault tolerant;
  - Another important property of the PIR is agent authorization; this property blocked the events that come from malicious agents which try to establish a direct communication to this module.
- Buffer and its controller;

5.3. Agents of Third Phase of Intrusion Detection Process

In this phase, processed events receive from the PIR and they will be considered. Each event verifies and sends to compare with existent policies into the policy-base. If a match found, conditions be evaluated; a right condition, it will trigger one or many actions; then, these actions forward to the response router. Now, events will be forwarded to the response server and be logged the activities of responders. This phase mainly dealing to the info-bases of processed events and taken actions by them and using the information of previous step; in attending to the following figure (**Figure 11**), the existent agents into this step are:

- Collector: this module gathers the ideas of corresponding WSN's components (such as sensor nodes) and enforcing decision making techniques such as majority rule.
- Responders: this agents are responding to the events; in other words, they trigger actions (in real-time).
- Response server (RS): processing triggered actions by responders. The actions that RS will trigger are: sending variety notifications, reconfiguration (firewall, IDS or its hosting-system), dropping, logging, trigger/stop services or in worst state, system shutdown.
  - RS is controlling the independent agents that trigger these responses. RS listen to the events that come from PIR to process them. RS has a dedicated agent-base; including information such as properties and address of responders;
  - Responder base or response-agent profile-base (if necessary, separated from RS): containing information about responder's agents' location; it is a profile of responder's agents;
  - Registering and controlling responders.
- Graphical user interfaces (GUI).
  - Displaying reports and graphs to the user.
- Dynamic Re-Config Agents (DRCA): if into the previous step be detected that the health of the WSNIDS or its hosting system has a trouble, this agent reconfigure and setting up them, again (such as updating Info-bases).
- Response logger (RL): logging total of responded incoming events and taken responses to them.
- Logging controller.
- Response router (RR): always alive state; this module participate into the intrusion detection process by en-

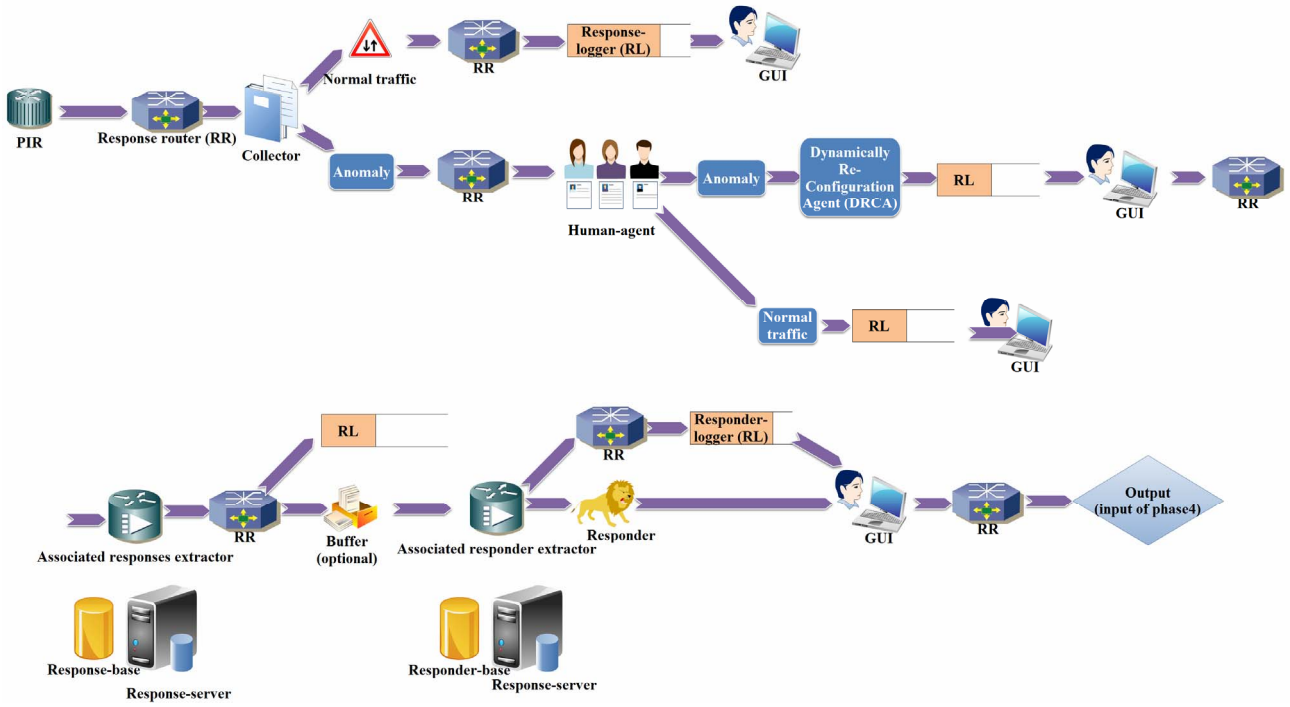


Figure 11. The third phase of intrusion detection process by WSNIDS: decision making and responding.

forcement decision making techniques, reacting and operating as a router and logger (routing and logging responses, agents' states, malicious events and processed events) and as an agent authorization (it allows renders to be trigger and react); besides routing, it activates other agents (if necessary and they be inactivated).

- Fault tolerant IDS: RR is a process which receives responses from RS, verified them and then, route them to their destination (next step and associated responder's agents). So the received events are into two categories: internal events (that come from the current step modules) and external events (they come from previous step). The PIR is able to take deterministic actions, independent from other agents; thus, it allows to the IDS that be fault tolerant;
- Another important functionality of the PIR is agent authorization; this property blocked the events that come from malicious agents which try to be intruded and established a direct communication to this module.

- Decision-info logger (DIL): logging the whole of taken decisions.
- Logging controller.
- Buffer and its controller.

5.4. Agents of Forth Phase of Intrusion Detection Process

According to the **Figure 12**, some of most important existent agents in this phase are:

- Logger: logging incoming data, processed data, decisions, responses and other information;
- Logging controller;
- Log Router (LR);
- Logs analyzer: some agents to analyze the log files of previous steps and then, extracting the required information to tracking;
- Tracker: this module can have more agents; for example, based on attack's nature;
- Graphical user interfaces (GUI);
  - Displaying reports and graphs to the user.

5.5. Types of Information Resources into the Proposed System

This phase is focused on logical data storage and different information resources (Info-bases) of the suggested system; according to the **Figure 13**, different types of required Info-bases into the intrusion detection process by the proposed system are:

- Policy bases: bases of rules which using to analyzing and intrusion detection; containing information such as policies (including events/data + conditions + responses/actions); it is including some relational tables such as responses table (including associated responses to key of each policy into the patterns table) and patterns table (table's fields are: source-node, current-node, previous-hop, next-hop, message-type, destination-node, data); types of policy bases are:
- Sensed info-base: the base of primary data, events and gathered auditing data to filtering and preprocessing; for example, system's log files and network traffic;
- Response/responder-base: including relational tables which they have fields such as agent-name, agent-id and hosting-system id;
- Config-info base: this base is containing information about normal setting and configuring the IDSs and their hosting systems; this information is using to reconfiguring and re-setting failure systems (if necessary); these information are using by IHHM module;
- tracking and forensic analysis information-base: including data to analyzing logs and then, tracking attackers;

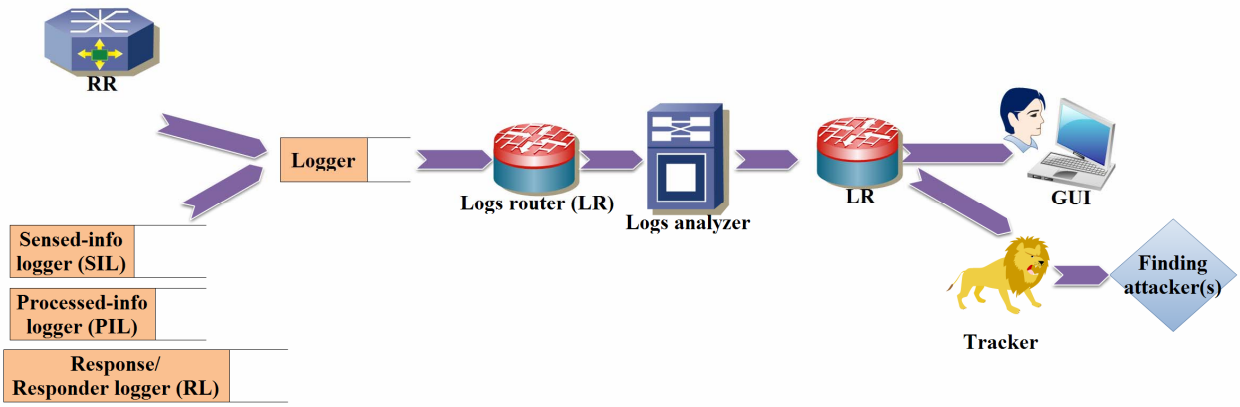


Figure 12. The forth phase of intrusion detection process by WSNIDS: logging and tracking.

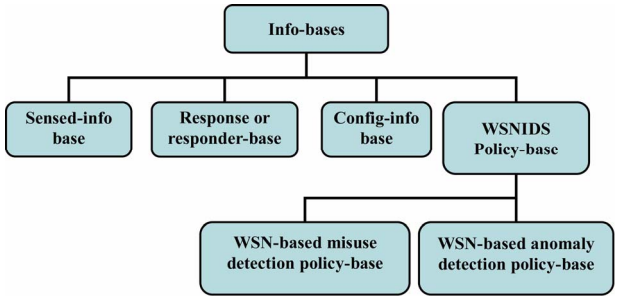


Figure 13. Different types of Info-bases into the proposed intrusion detection system.

- Policy bases of the sink:
  - WSNIDS-based misuse detection policy-base: containing patterns of known attacks to detecting based on signature;
  - WSNIDS-based anomaly detection policy-base: including patterns of normal traffic to detecting anomalies.

Following figure (**Figure 14**) is showing the data flow into the WSNIDS, in more detailed. As shown **Figure 7**, **Figure 8** and **Figure 14**, the WSNIDS is based on analyzing auditing data, detecting malicious traffic and concluding the WSN's behaviors. The taken approach in the WSNIDS has following features:

- 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 responding layer, tracking and forensic analysis layer; also, it has a user interface in different layers.

5.6. The Main Properties of the WSNIDS

The suggested system has following features:

- Modularity and high-flexibility; *i.e.* possibility to adding new plugins such as third-party detectors and third-party detection engines;
- Scalability;
- Dynamic reconfigurable, fault tolerant and robustness;
- Safety against unauthorized access;
- Ease of extensibility;
- Efficiency, high performance, optimal energy consumption and increase the WSN lifetime and its stability;
- Independence and autonomous phases and their agents; they have dependency to each others.
- Powerful detection process (since there is the WSNIDS on the sink, proper policies and rules and comprehensive Info-bases);

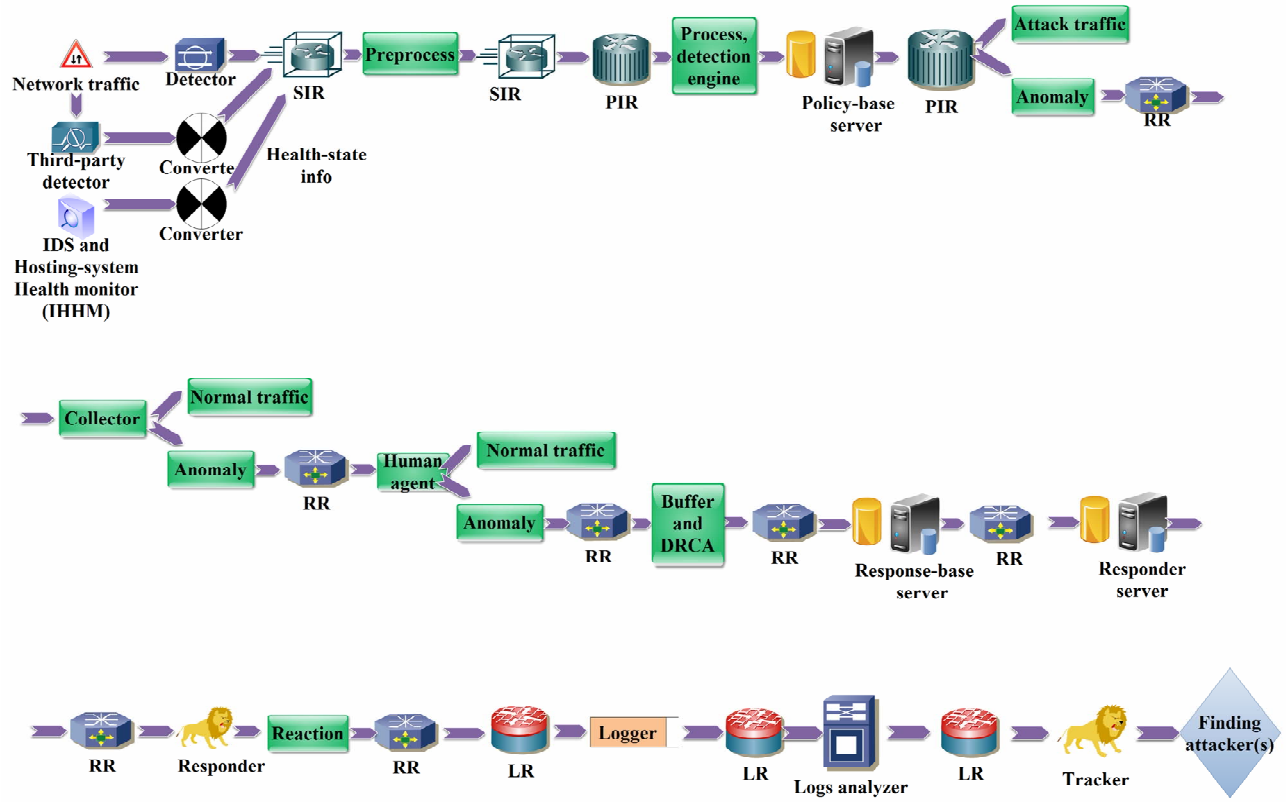


Figure 14. The WSNIDS data flow.

- The WSNIDS is based on agent and policy;
- It allows to use authentication and authorization mechanisms for different phases of the WSNIDS; for example, SIR to the PIR, to establishing secure communications between different phases (and their agents) and preventing from intrusion of unauthorized agents;
- 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; *i.e.* the used matching function);
- Shared activities of the WSNIDS's agents: Some of common operations of agents in different intrusion detection phases are:
  - Authorization: to preventing from intrusion of unauthorized agents;
  - Authentication: to preventing from intrusion of unauthorized agents;
  - Routing;
  - Logging.
- Fault tolerant and dynamic reconfiguration:
  - Using backup network equipments, such as sensor nodes; *i.e.* there are some backup sensor nodes;
  - Using backup agents into the WSNIDS;
  - Predicting the location deployment of back up sensor nodes in the WSN;
  - Existing dynamic reconfiguration agents for the WSNIDS and its hosting system;
  - 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 notification or warning type once an event occurred;
- Security considerations:
  - The WSNIDS protection (monitoring the health state of the WSNIDS and its hosting system, continuously) and stability of hosting system of the WSNIDS;
  - This architecture is dependence to the network data flow;
  - There is logging capabilities.

6. Result

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 WSNIDS; 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 of 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. Pre-processing and Processing Properties

As **Table 1** is showing, the proposed architecture supports different dimensions of IDSs' processing properties. For example, the WSNIDS's monitoring level is almost 96 percent; *i.e.* it covers the WSN's components such as sensor nodes, almost completely. Also, the extendibility capability of the WSNIDS is about 82.7 percent. Besides, the WSNIDS has dynamic re-configurability capability about 66.9 percent. It is evaluated the WSNIDS is including the properties of processing and managing category about 81.87 percent, in average.

6.2. Operational Properties

Table 2 is representing the different aspects of the WSNIDS's operational requirements. According to the following table, the WSNIDS supports real-time detection property almost 80.6 percent. Also, it has the content-based (body of a packet) detection and context based

Table 1. Processing properties of the WSNIDS.

No.	Question	Functional properties		Non-functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Monitoring level	-		96
2	Extendibility and flexibility	-		82.7
3	Dynamic re-configurability capability	-		66.9
	Average (percentage)	-		**81.87**

Table 2. Operational properties of the WSNIDS.

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	-		80.6
2	Content-based detection capability	-		89.4
3	Context-based detection capability	-		55.7
4	Supporting multiple platforms and multiple OS	Yes		-
5	Automatic reaction to the intrusions	Yes		-
	Average (percentage)	-		**75.23**

(header of a packet) detection capabilities about 89.4 and 55.7 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 reacts to the attacks, automatically. Finally, the WSNIDS is included the properties of this IDSs' requirement category about 75.23 percent, in total.

6.3. Output Requirements

Following table (**Table 3**) shows the WSNIDS 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

Table 4 is representing and questioning the WSNIDS's technical properties. For example, ease of implementation of the proposed system is evaluated about 85 percent; the WSNIDS has fault tolerant, scalability and robustness capabilities, each one almost 74, 92.5 and 64.2 percent, in order. Besides, the WSNIDS is an efficient system; since it does not enforce extra load to the WSN re-sources and its normal functionalities. As a result, the proposed architecture supports different properties of this IDSs' requirement category about 78.48 percent, in average.

6.5. Special and High-Level Properties of the WSNIDS

Following table (**Table 5**) represents and considers the required especial and high-level properties of the WSNIDS. As the acquired result of the questionnaires shows, the proposed system has modular and flexible architecture. The WSNIDS is included centralized management on the WSN resources (such as info-bases) and its components. 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. This architecture supports accurate management of resources, non-enforcing extra load to the WSN and monitoring the health state of the WSNIDS and its hosting system. The proposed system is a secure architecture; *i.e.* it is resistant and robust against attacks. The WSNIDS has centralized control on inter-components data communications and interactions from the sink, by user. This system can detect chaining attacks by using powerful detection process and audit trial mechanisms (about 64.8 percent). The WSNIDS is evaluated as an optimal system in energy consumption; since, it is attending to the energy consumption in designing step (almost 75.6 percent). The strength of detection process on the proposed system is evaluated about 89 percent (because there is strong and big info-bases and hierarchical detection process). The WSNIDS has attention to taking back-up designs; *i.e.* it supports the back-up components and performs operations such as buffering. The WSNIDS's efficiency and its functionality are depending on to the network data flow; its dependability is evaluated almost 87.5 percent. The suggested architecture is consistent to the centralized and autonomous operations in WSNs; its consistency is evaluated about 88.2 percent. The proposed system is providing the possibility of updating and configuring network components from a central control location; *i.e.* it is possible to configure sensor nodes from the sink (*i.e.* deployment location of the WSNIDS). Ease of updating and integrating new capabilities and new functionalities to the proposed system is almost 85.5 percent. It is also possible to update the WSNIDS and its operational using, simultaneously. As a result, the WSNIDS is included different properties of this IDSs' requirement category

Table 3. Output properties of the WSNIDS.

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 WSNIDS.

No.	Question	Functional properties		Non-functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Ease of implementation	-		85
2	Fault tolerant capability	-		74
3	Scalability	-		92.5
4	Robustness	-		64.2
5	Safety (against unauthorized access)	-		76.7
6	Enforcing extra load to the WSN	No		-
	Average (percentage)	-		**78.48**

almost 80.86 percent, in total.

7. Conclusions

The purpose of this paper is considering intrusion detection issue on WSNs and designing an Intrusion Detection System (IDS) for these networks (the WSNIDS), 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 four phases; including: monitoring and pre-processing, processing and analyzing, decision making and responding and finally, logging and tracking. The main attributions of the suggested architecture are as following:

- Major properties of the WSNIDS: based on agent and policy, independent and autonomous agents, strong and comprehensive info-bases, dynamically reconfigurable, scalable, component-based and modular, high-flexibility and network-based architecture;
- Robustness and fault tolerant design;
- Ease of extensibility;
- Detection method:
  - Combinational (*i.e.* based on signature and anomaly);
  - Centralized (by the WSNIDS on sink);
- Decision making approach: combinational;
  - About each sensor nodes, the WSNIDS makes decision, independently and autonomously;
  - About anomaly occurrence, the WSNIDS and if necessary, human agents make final decision, cooperatively.
- Response method: combinational; *i.e.* active response and passive response, depend on conditions and 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, the WSNIDS is very near to attacker (one-hop distance);
- Matching and multi-agent detection process to detecting attacks along with low error rate;
- The heterogeneous WSN;
- Consistent with automatic, autonomous and independent mechanisms of WSNs;
- Possibility of centralized management on the WSN, systems and their resources;
- Focused on routing layer;
- According to the **Table 1**, **Table 2**, **Table 4** and **Table 5**, following table (**Table 6**) is representing integrated average values of different IDSs' requirement classes;
- According to the **Table 6**, following figure (**Figure**

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

No.	Question	Functional properties		Non-functional properties
		Yes	No	In percentage (0 - 100) : Total average
1	Modular and flexible architecture	Yes		-
2	Centralized management on the WSN	Yes		-
3	Minimize resources property	-		66.3
4	Accurate management of resources and monitoring the health state of the WSNIDS and its hosting system	Yes		-
5	The WSNIDS security	-		67.5
6	Centralized control on inter-components data communications	Yes		-
7	Ability to detecting chaining attacks	-		64.8
8	Attending to the energy consumption	-		75.6
9	Strength of detection process	-		89
10	Possibility to taking back-up designs	Yes		-
11	The WSN data flow dependability	-		87.5
12	Consistency to the centralized and autonomous operations of the WSN	-		88.2
13	Existing different control locations	Yes		-
14	Ease of updating	-		85.5
15	Possibility to updating the WSNIDS and its operational using, simultaneously	Yes		-
	Average (percentage)			**80.86**

Table 6. Total average value of different properties category.

No.	Properties class	Total average value (in percentage)
1	Preprocessing, processing and managing properties	81.87
2	Operational properties	75.23
3	Technical properties	78.48
4	Special and high-level properties	80.86
	Average value (in percentage)	**79.11**

15) is formed. **Figure 15** is showing the sum average values of different IDSs' properties categories; in other words, the WSNIDS supports different categories of IDSs' required properties (as **Figure 15** shows);

- As above figure shows, the processing and managing properties of the suggested system has been assessed almost 81.87 percent, in average; *i.e.* the WSNIDS supports different aspects of this requirement category about 81.87 percent. Also, the supported operational and technical properties by the proposed architecture have been evaluated about 75.23 and 78.48 percent, in order. The proposed system is included especial and high-level required properties of IDSs almost 80.86 percent, in general. As a result, the proposed system is included different IDSs' requirement categories almost 79.11 percent, in total average.

In summarize, the posed system in this paper is a comprehensive model which has some main properties such as robustness, scalability, extensibility and incremental matching along with environment changes and its new conditions. Also, the WSNIDS is focused on integrating the accessible tools in security area of computer networks (like IDSs, logging, tracking and forensic analysis systems). This architecture is a distributed model for intrusion detection on WSNs. It is hoped to this research able us to improving the security level of WSNs.

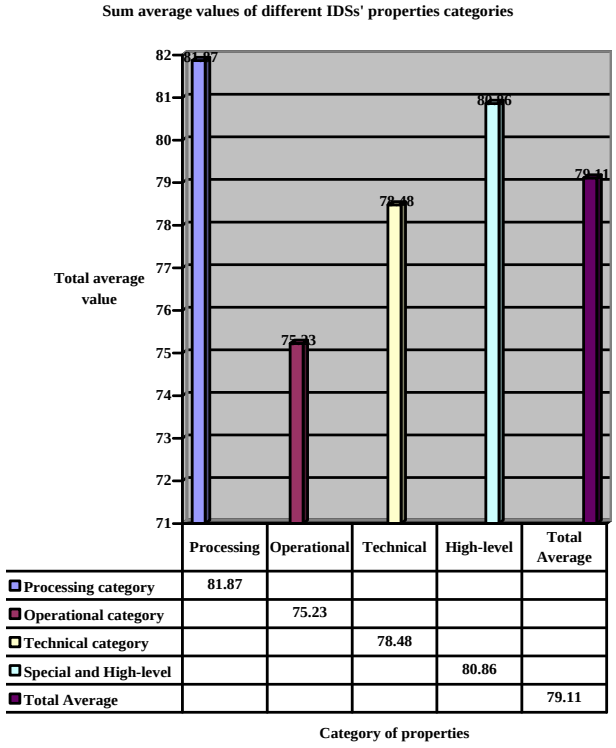


Figure 15. The sum average values of different requirements categories of IDSs.

8. Future Works

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

- Approaches to improving response scheduling, priority responses and having more control on response production mechanism;
- Methods for providing higher level of security, fault tolerant and robustness for suggested architecture;
- Preparing more detailed information about system activities for forensic analysis;
- Efficient data management;
- Developing user friendly interfaces which allow dynamic reconfiguration of systems and representing the activities of these systems, in graphical;
- Methods for minimal and optimization energy consumption and network delay in WSNs;
- Approaches for data aggregation in WSNs;
- Key management mechanisms on WSNs;
- Techniques for using of mobile nodes in WSNs;
- Approaches to extending the proposed architecture (in different dimensions such as security);
- Implementing the WSNIDS.

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," *Journal of Information Assurance and Security*, Vol. 6, No. 1554-1010, 2011, pp. 195-215.

[2] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," *Journal of Information Security*, Vol. 2, No. 2, 2011, pp. 69-84. doi:10.4236/jis.2011.22007

[3] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," *International Journal of Computer Applications*, Special Issue, 2010.

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

[5] M. Saxena, "Security in Wireless Sensor Networks: A Layer-Based Classification," Department of Computer Science, Purdue University, West Lafayette.

[6] Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks," Department of Electrical and Computer Engineering, University of Waterloo, Waterloo.

[7] A. Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN," Department of Computer Science, Faculty of Electrical Engineering and Information Technology, Republic of Macedonia, Skopje.

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

[9] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Berkeley, 11 May 2003, pp. 113-127. doi:10.1109/SNPA.2003.1203362

[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler and D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, Vol. 8, No. 5, 2003.

[11] L. Krishnamachari, D. Estrin, and S. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," *Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops*, 2002, pp. 575-578. doi:10.1109/ICDCSW.2002.1030829

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

[13] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology, February 2007, pp. 800-894.

[14] G. Maselli, L. Deri and S. Suin, "Design and Implementation of an Anomaly Detection System: An Empirical

Approach," University of Pisa, Pisa, 2002.

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

[16] Ch. Krügel and Th. Toth, "A Survey on Intrusion Detection Systemsm," Vienna University of Technology, Vienna, 2000.

[17] J. Molina, "Evaluating Attack Resiliency for Host Intrusion Detection Systems," Doctoral Dissertation, University of Maryland, College Park.

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

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

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

[21] S. Zanero and S. M. Savaresi, "Unsupervised Learning Techniques for an Intrusion Detection System," *Proceedings of the* 2004 *ACM symposium on Applied computing*, Nicosia, 14-17 March 2004, pp. 412-419.

[22] O. Depren, M. Topallar, E. Anarim and M. K. Ciliz, "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks," *Expert Systems with Applications*: *An International Journal*, Vol. 29, No. 4, 2005, pp. 713-722. doi:10.1016/j.eswa.2005.05.002

[23] R. A. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," Computer Science Department, University of California, Santa Barbara, 2002.

[24] 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

[25] 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.

