A HIERARCHICAL INTRUSION DETECTION ARCHITECTURE FOR WIRELESS SENSOR NETWORKS

Hossein Jadidoleslamy
Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, Iran
tanha.hossein@gmail.com

ABSTRACT

Networks protection against different types of attacks is one of most important posed issue into the network and information security application domains. This problem on Wireless Sensor Networks (WSNs), in attention to their special properties, has more importance. Now, there are some of proposed architectures and guide lines to protect Wireless Sensor Networks (WSNs) against different types of intrusions; but any one of them do not has a comprehensive view to this problem and they are usually designed and implemented in single-purpose; but, the proposed design in this paper tries to has been a comprehensive view to this issue by presenting a complete and comprehensive Intrusion Detection Architecture (IDA). The main contribution of this architecture is its hierarchical structure; i.e., it is designed and applicable, in one or two levels, consistent to the application domain and its required security level. Focus of this paper is on the clustering WSNs, designing and deploying 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 and clustering structure, clusters' overlapping and using hierarchical routing protocol such as LEACH, but along with minor changes. Finally, the proposed idea has been verified by designing a questionnaire, representing it to some (about 50 people) experts and then, analyzing and evaluating its acquired results.

KEYWORDS

Wireless Sensor Network (WSN), Security, Routing, Intrusion Detection System (IDS), Attack, 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 compose 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 stations" (i.e. central server and the WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes [1, 2]. As shown in Figure1, aggregation points collect information from their nearby sensors, integrate and aggregate them and then forward to the base stations to process gathered data. 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, security is a vital and complex requirement for these networks. In attending to the WSNs' constraints, their requirements and unusable traditional network security techniques on WSNs [2, 3]; so the defensive-security mechanisms 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; of course, by attending to the existent obstacles and constraints in these networks. Our proposal is adding a another defensive line, called Intrusion Detection System (IDS), as a new defensive-security level to the WSNs' security infrastructure; which it can detects unsafe activities and unauthorized login/access, and when attacks occurred, even new attacks such as anomalies, it can notifies by different warnings and operates required actions (mainly predefined actions). Therefore,

DOI : 10.5121/ijnsa.2011.3511

the main purpose of this paper is presenting, discussing and solving the intrusion detection problem in WSNs. This paper by focus on WSNs' security follows this goal, including:

- An overview of WSNs and their security;
- Discussing Intrusion Detection System (IDS) as a new aggressive-defensive security layer for WSNs;
- Suggestion a comprehensive, hierarchical and distributed intrusion detection model and IDS architecture on WSNs (CIDS and WSNIDS architectures);

This paper makes us enable to identify the existent security challenges in WSNs and we can almost solve intrusion detection problem in these networks, by adding a new defensive-security layer, called IDS, to WSNs' security infrastructure; 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 important and different dimensions, and IDS 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) for WSNs; Section 6 prepares a questionnaire to verifying the IDA; Section 7 expressed the reached results and conclusion; and finally future works, some proposed topics to research, are drawn in section 8.

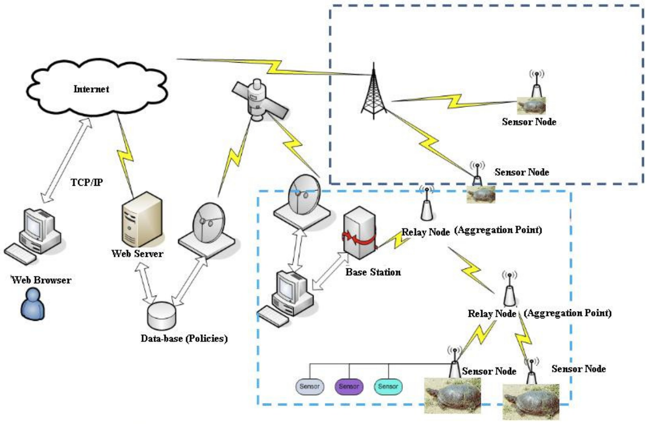


Figure 1. WSNs' communication architecture

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]. Major features of WSNs are:

- Infrastructure-less [1, 2] and no public address, often (data-centric network) [2, 5];
- Consisting of many (hundreds or even thousands) tiny sensor nodes [2, 4, 10];
- High-density of nodes distribution [6] (in operational environment);
- Insecure radio links;
- Application-oriented networks;
- Different communication models [1, 2, 8], including: hierarchical/distributed WSNs; or homogenous/heterogeneous WSNs;
- Limited resources of sensor nodes [5, 6, 9];
- Having decision making capability to react to the events;
- Main application domains of WSNs are: monitoring and tracking (as shown in Figure2); therefore, some of the most common applications of these networks are: military, medical, environmental monitoring, industrial, infrastructure protection, agriculture, intelligent buildings and transportation.

The taken approach in 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 characteristics, architecture, vulnerabilities, different security dimensions and routing.

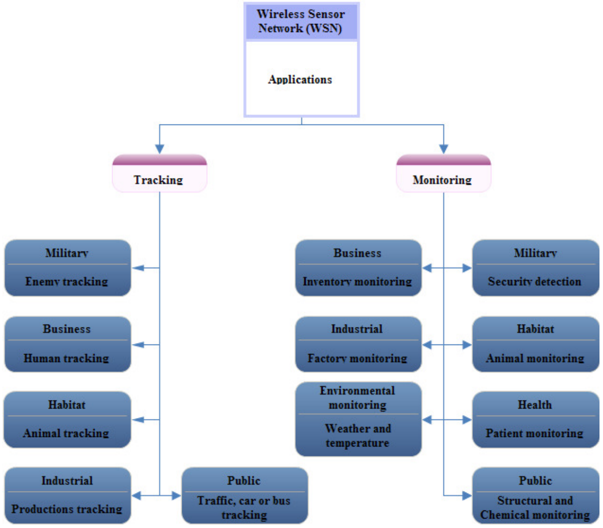


Figure 2. WSN's applications

2.1. WSNs characteristics

A WSN is a homogenous or heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors to monitor and gather real-time information from deployment environment [2, 7]. Common functionalities of WSNs' nodes are broadcasting and multicasting, routing, 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 Figure3. Some of most important characteristics of these networks are:

- Wireless and weak connections [1, 3, 8];
- Low reliability of sensor nodes;
- Dynamic topology and self-organization [2, 4] (unpredictable WSN's topology);
- Ad-hoc based networks and hop-by-hop communications (multi-hop routing);
- Open/hostile nature of deployment environment [2, 5, 9];
- Inter-nodes broadcast-nature communications [3, 7];
- Ease of extendibility (scalability);
- Direct communication, contact and interaction with physical environment [1, 6];
- Putting down and consistency capabilities of sensor nodes (on different environments);
- Automatically [4, 10] and non-interrupted operation [5, 6];

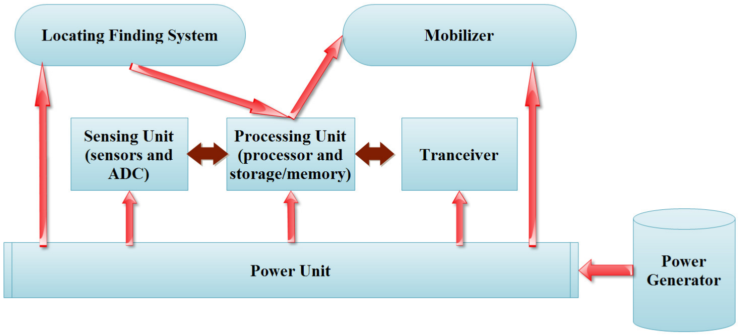

Locating Finding System
Mobilizer
Sensing Unit (sensors and ADC)
Processing Unit (processor and storage/memory)
Tranceiver
Power Unit
Power Generator

Figure 3. WSN's node architecture

2.2. Different types of WSNs' architectures

As shown in Figure4, on WSNs' architecture, there are components such as sensor nodes (motes that are sensing data), aggregation points (cluster-heads), base stations [1, 2] (central server), network manager, security manager, and user interface [8, 10]. These components participate to each other; thus, they help to the WSN to operate, correctly. Figure4 shows different kinds of WSN's architectures.

2.2.1. Direct communication architecture

- Each sensor nodes communicates to the sink (central server), 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];
- 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: the weakness of this architecture is: most communication operations are doing by cluster-heads; thus, their energy will be consumed, decreased 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;

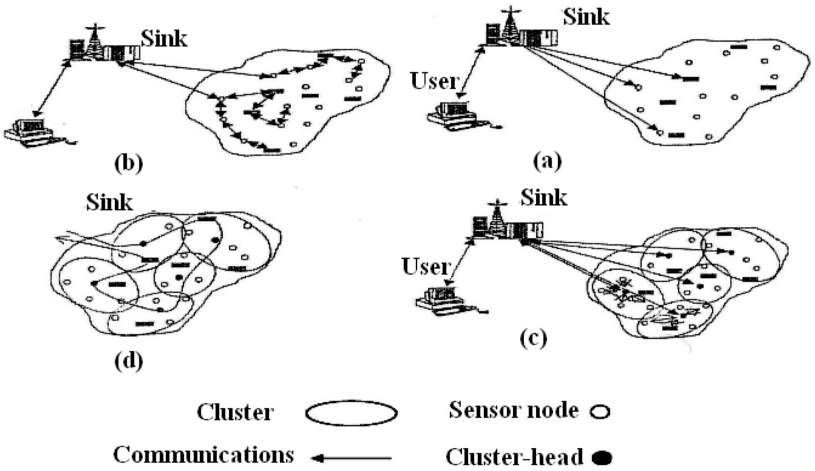


Figure 4. Different types of WSNs' architectures: (a) Direct communication architecture; (b) Multi-hop and peer-to-peer architecture; (c) Multi-hop based on clustering architecture; (d) Multi-hop, clustering and dynamic cluster-heads architecture;

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, compromising and replicating) [3],
- 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 and capture nodes);
- Insider attackers (internal attacks);

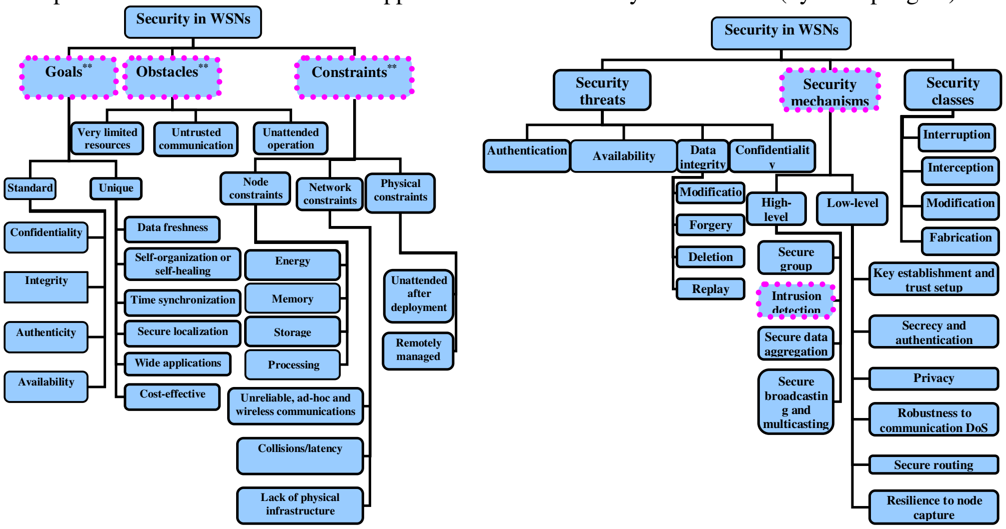
- Inapplicable and un-usability traditional network common security techniques [2, 3];
- Requirement to redesigning security architectures and protocols (distributed and self-organized);
- Unreliable communication [2];
- Vulnerability and susceptibility against eavesdropping;
- Unattended nature and operation [1, 2];
- Dynamic structure, unpredictable topology and self-organization [1];
- Sensor nodes' selfishness [2, 7];
- Requiring to forwarding and routing sensed information to a shared destination, called sink;
- Existing redundancy in gathered traffic;
- Fault tolerant [1, 7];

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. 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 untrusted sensor nodes [1, 4];
- Requiring trusted center for key management, to authenticate nodes to each other [1, 6, 9];
- Broadcast and wireless nature of transmission media [1, 3];
- Sensor nodes deploy on hostile environments [1, 7] (unsafe physically);
- Unattended nature and operation of WSNs [1, 2, 10];

Some of most important dimensions of WSNs have been shown in following figure (**Figure5 (a) and (b)**) by star spangled (starry boxes). As **Figure5 (a)** shows, in this paper we have emphasize on goals, obstacles and constraints of WSNs' security aspects. Also, **Figure5 (b)** is showing which this paper has been emphasized on intrusion detection approach from the security mechanisms (by star spangled).



(a)

(b)

Figure 5. Security in WSNs

2.5. Routing in WSNs

2.5.1. Effective parameters on designing WSNs' routing protocols

Some of most important desirable criteria in designing WSNs' routing protocols are:

- WSNs' variable and different configurations and dynamic topology;
- Different addressing design;
- Method of sensor nodes' deployment on the WSN;
- Amount of energy consumption/waste [8, 11];

⇨ The most important issue in designing WSNs' different protocols, like routing protocols, is the cost of energy consumption factor. On WSNs, each node usually consumes energy to measure the goal parameter (gather information), transmit and process the raw data. But, the step of data transmission consumes more energy than others.

- Used data transmission and reporting method [9, 10]: this is including following models; i.e. time-driven model, event-driven model, query-driven model and combinational model;
- Data aggregation;

⇨ In attending to the most energy consumption step of the WSN's processes is data transmission, protocols designers usually try to using data aggregation and processing, compression, compaction and combination techniques to decrease the volume of sent data (before forwarding it).

- Quality of Services (QoS);
- Fault tolerant [8];
- Scalability;
- Node development and it's especial characteristics, such as limited resources;

⇨ Routing protocols should monitor, control and manage the resources of nodes and the WSN, in accurate;

- Consistency with operating environment;
- Matching with communication channel frequency and transmission media;
- Fairness;

2.5.2. Types of WSNs' routing protocols

According to the Figure6, routing protocols of WSNs. depend on the network nature and its structure, can be classified as follows:

- Data-Centric routing protocols: These kinds of WSNs' routing protocols operate as do not make send much repeated data [8]; in other words, these protocols want to reduce data redundancy and prevent from forwarding repeated data.
    - o Data naming and requests, based on network specifications and application domain [11];
    - o Query-based (queries come behalf on the base station or central server);
    - o No requirement to node clustering;
- Hierarchical routing protocols:
    - o The WSN clustering [9, 11];
    - o Independent and autonomous clusters [10, 12] (clusters are and operate independent than each other);
    - o Cluster-head selection for each cluster, to does functions such as receive and gather corresponding cluster nodes' data, aggregate them, reduce repeated data, forwarding and routing them to the base station;
    - o Types of cluster-heads are: similar to the WSN or corresponding cluster nodes (homogenous network) or non-similar than typical the WSN or corresponding cluster nodes which have different hardware and software resources, capabilities and powerful (heterogeneous network);

    ⇨ This approach is used on the proposed WSN and Intrusion Detection Architecture (IDA) (as shown in Figure6) by star spangled.
- Location-based routing protocols:
    - o Using information of nodes' deployment location to find optimal routes to information transmission and efficient routing [9, 10];
- Network-Data Flow routing protocols;
- QoS-based routing protocols:
    - o They used on applications which must attend to other parameters, such as QoS, besides of energy consumption/waste [8, 9, 12];
    - o Example: applications which sensor nodes have to transmit audio or video;

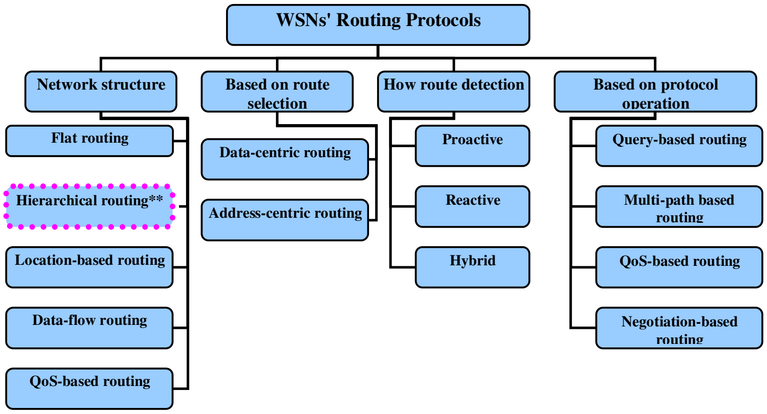


Figure 6. Routing in WSNs

2.5.3. Hierarchical routing protocols (clustering-based)

One of most important design parameters of WSNs is scalability [8, 9]. Suppose that all of WSN's traffic volume be routed by one or more specific routes; so, the WSN's performance will be reduced; due to some reasons, like network widespread, WSN's traffic growth and its delay. Thus, according to the sensor nodes' limited radio range and their constraints on remote communication (they usually do not have remote communication capability), using such method can be limited the WSN's extensibility. Therefore, the clustering techniques have been proposed; since these methods can increase the WSN coverage area (more and wide), without reduction the QoS of the WSN's services [10]. The main purpose of hierarchical protocols is using appropriate method to consume energy resources, optimally [11, 12]. To reach to this goal, these protocols are using multi-hop routing to forward and transmit data into the WSNs and cluster-heads aggregate information of their corresponding cluster nodes to compress and reduce the volume of sent data. The LEACH[1] protocol is the first hierarchical routing protocol(s) which has been designed for WSNs and it is base of many other WSNs' routing protocols. As shown in Figure6 and Figure7, the taken approach for routing in the WSN and proposed IDA is hierarchical, which using LEACH hierarchical routing protocol, especially; of course, along with a little changes. In resume, we will describe the LEACH routing protocol.

2.5.4. The LEACH routing protocol

The LEACH protocol is a self-organized protocol along with dynamic categorization, which using a random method to distribute energy consumption between each clusters' nodes [9, 10]. In this protocol, time divide into slots, called round; then, rounds and their operations are repeated, in periodic. Each round can be divided into two phases, including: setup phase (clusters formed) and stable state phase (the WSN normal functionality) [8, 9].

In first phase, based on a matching probabilistic function, cluster-heads be selected [11] (i.e. each node choose a random number between 0 and 1; then, if the selected number be less than a predefined threshold value, that node will be chosen as cluster-head, in the current round duration). The probability function has been designed as in during specific rounds; each node only once can be cluster-head (only one time). Consequently, energy consumption is distributed on the WSN's wide level. Then, after choosing and determining cluster-heads, each cluster-head broadcast a message to introduce and advertise itself to other nodes as a cluster-head (using CSMA MAC techniques) and each node also select an appropriate cluster-head for itself, based on parameters like requirement energy for data transmission, energy consumption and received signal strength (to forming clusters) and then, notify and inform it to the corresponding cluster-head [10, 12]. Now, each cluster-head setting up a scheduling program for corresponding cluster nodes and it allocates a time slot to each sensor node to transmit their data and preventing from collision between packets of inter-cluster nodes (using CDMA techniques). Also, we can use the DSSS[2] method to preventing from collision between different clusters' data (as shown in Figure7).

In second phase, each node sends its data on its assigned time slot and then cluster-head after receive total associated cluster nodes' data, it aggregate them and forward to the base-station [11, 12]. In attending to

[1] Low-Energy Adaptive Clustering Hierarchy (LEACH)

[2] Direct Sequence Spread Spectrum

each cluster-head aggregate and combine all corresponding cluster nodes' data, make reduction of sent data volume (to the base-station) and consequently, reduce and save energy consumption. Therefore, it can prevent from energy waste and nodes' battery evacuation (according to the Figure7).

⇨ In different rounds, the LEACH protocol is selecting and using cluster-head in random and dynamic rotation/change between corresponding cluster nodes, which have more energy than others; so, it prevents from nodes' battery evacuation and energy loss of specific nodes than others. Besides, this protocol using local data fusion to compress sent data from clusters to the central server (base station); thus, this work reduces the requirement energy to broadcasting information and as a result, it will increase the system useful lifetime.

⇨ The probability of a node selection as cluster-head is proportional to the node's remained energy (into that node's battery).

⇨ Clusters and their corresponding nodes change in different rounds.

⇨ The optimal number of clusters can be determined based on some parameters such as the network topology and processing (communication and calculations) cost; some of research in this field shows the appropriate number of cluster-heads in a WSN is almost 5 percent of whole nodes.

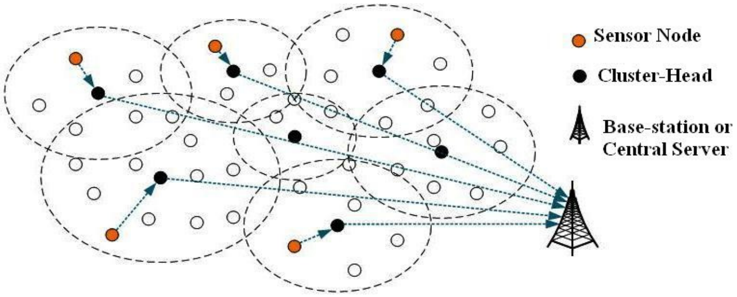


Figure 7. The LEACH hierarchical routing protocol

2.5.5. Details of the LEACH routing protocol

In summarize the steps of the LEACH protocol are:

- Advertising phase: determining cluster-heads;
- Clusters formed phase: informing to the selected cluster-head by the sensor nodes, using CSMA MAC methods (in this phase, the receiver of all cluster-heads should be on);
- Scheduling phase: creating TDMA scheduling programs by cluster-heads and notifying them to the corresponding clusters' nodes (in broadcasting method on cluster level);
- Data transmission phase: starting information transmission; so, cluster-heads receive messages from corresponding clusters' nodes, based on the scheduling program; then, compressing and aggregating total received data in form of a unit signal with using signal processing operations by cluster-heads; finally, sending conclusive signal to the central server;

⇨ Proposed approach: constant and static cluster-heads and clusters through network lifetime.

2.5.6. Specifications of the LEACH routing protocol

Main specifications of the LEACH protocol are:

- Idea: clustering sensor nodes, dynamically (lead to increasing network lifetime and reducing the difference between different nodes' lifetime);
- Problem: waste and loss energy (to forming clusters, in start of each round);
- The performance of this protocol's functionality is proportional to nodes density (there is a direct proportion between the protocol's functionality performance by/and nodes' density);
- Requiring minimal energy to transmit data (because this protocol does operations such as data filtering, data collaborative and parallel processing [8, 9, 11], in-network data aggregation and caching information [11, 12]).

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 Figure8, Intrusion Detection Systems (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 [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 them (network traffic) in sophisticated, to finds attacks traffic (it does complex analysis on network traffic to find malicious traffic) [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 total network traffic [19];
- Capturing the transmitting network packets [20];
- 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 appropriate 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 station;
- Based on distributed and heterogeneous resources [14, 15, 18];
- High complexity, variable specifications and agent-based.

As a result, 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 appropriate 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.

⇨ In the proposed architecture, sensor nodes are partitioned as some clusters; each cluster has a cluster-head and any cluster-head 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 other to complete the intrusion detection process. They can use the simple majority vote rule to make an appropriate decision.

3.2. IDS classification based on detection method

IDSs must be able to differentiate between normal and abnormal activities (traffic), to detect malicious efforts, in real-time. As Figure8 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 centralized on normal behavioral patterns [14, 15]. According to the expert systems are not able to timous update models and patterns, we will need to 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 determine and differentiate attack traffic, easily. In this approach, it is possible 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;
    - Events which have severe deviation from defined statistical values of these patterns ⇨ abnormal behaviors and intrusion efforts;

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

3.2.2. Signature-based Detection Systems

This method is using deterministic scenarios, patterns and rules 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 details. 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] of known attacks into the IDS;
- Necessity of adding new patterns of attacks to the patterns' set (info-base), manually and repeatedly;

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

⇨ 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 (less effective to use of them 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 (in form of pattern) 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 central server and highest level, and CIDSs on cluster-heads.

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 (rapidly); because the network is clustering, CIDSs are distributed as cover total nodes of the network; then, corresponding CIDS is near to the attacker (on single hop distance).

⇨ It is possible to detect in 1 or 2 levels; i.e. if CIDS can not detect attack or make decision about attack occurrence or its policy-base do 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, we want to discuss about who should make final decision on 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 Figure8, 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 (a suspicious node), decision making also should be cooperative (again) [13, 15]; 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, central server (WSNIDS), should take appropriate decisions by participate to each other.

3.3.2. Autonomous and independent mechanism

In this method, cluster-heads take decisions, autonomously [16, 17]; they gather evidences and criteria of anomaly and intrusion activities from other co-cluster nodes and then, make decision on 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 cluster-heads is weak [12, 13] (of course, in homogenous WSNs); attackers can compromise them soon and easy; therefore, this leads to loss of the network control.
- Enforcing excessive computational and processing overhead on cluster-heads; therefore, in attending to limited resources and being few key nodes, on homogenous WSNs, lead to their lifetime reduction (energy 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 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, cluster-heads make decision about intrusion occurrence and proportional actions; if necessary, they cooperate to each others (for example, in case of boundary nodes). i.e., the WSN's nodes be clustering and forming clusters; in each cluster, the cluster-head gather the data from other corresponding cluster's nodes, then form and maintenance a machine state for any one of them; then, cluster-head (CIDS) can take appropriate and conclusive 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, corresponding cluster-head make decision on intrusion to its co-cluster nodes. Also, 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, central server (WSNIDS) takes final decision about attack occurrence and appropriate reaction.

⇨ In suggestion approach, at first level, cluster-heads make decision on attack occurrence to a sensor node 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 cluster-heads deploy in each other and central server (WSNIDS) radio communication range; i.e. each cluster-head place in the radio communication range of neighboring cluster-heads and central server; 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 (shared nodes in neighboring clusters and they are into radio range of neighboring cluster-heads) can have a safer and more reliable conclusion by using and enforcing 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 (inactive) or the central server must be notified and take appropriate decision about it". It means, if a boundary node has been n neighboring 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 (in decision making process) 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.

3.4. IDS categorization based on reaction method

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

3.4.1. Active Reaction

These responses prevent from the attackers' activities, directly [13, 16]; for example, session disconnection [19], dynamic reconfiguration of the network equipments, using Honeypot, 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 error importance).

3.4.2. Passive Reaction

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 WSN: using combinational method; i.e. active and passive responses by each others, depend on conditions, type and nature of attacks; thus, the type of response be determine proportional to 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.

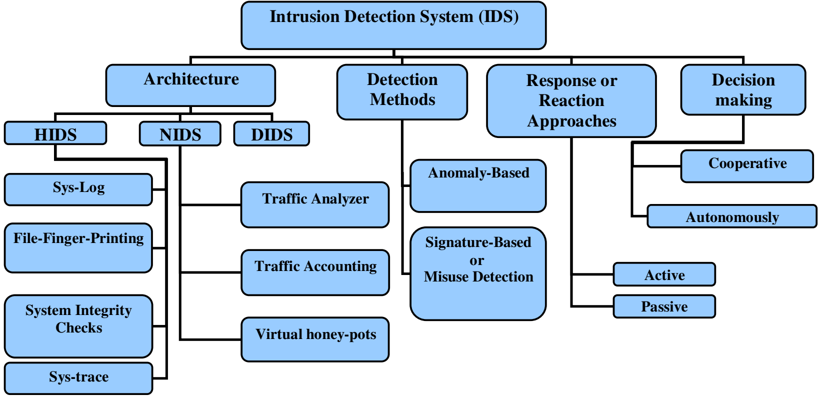


Figure 8. Different categorizations of IDSs

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 used and 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 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, 5, 9, 13];
- Repeated failures and unreliable sensor nodes;
- Application-oriented networks [8];
- 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; it is difficult to using protocols that are rely on time synchronization;
- Databases challenges: the volume of gathered data in the dynamic WSNs is very; storage medium; supporting different queries from nodes, cluster-heads and the central server; data indexing and local queries to perform queries faster; fast input of new data; fast changes of data; requiring fast and real-time updates; enforcing very costs through changes and communications; weak of data freshness;

4.2. The basis requirements of IDS in WSNs

In this section, we will describe the basis requirements of IDS for WSNs; i.e. we want to describe 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]. Therefore, an optimal and appropriate solution to solving this problem is architecture by following properties:

- Distributed and based on cooperation of nodes, cluster-heads and central server;
- Localize auditing: IDS of WSNs should operate by using local and minor auditing data (such as CIDS, in the same cluster level); thus, distributed approach for these networks is appropriate and consistent (an accurate and comprehensive monitoring in cluster wide level, preprocessing, analyzing and processing).
- Minimize resources: IDS for WSNs has to consume low dose of nodes' and/or 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: accurate management of resources, lack of non-enforcing extra load to the WSN, performance and monitoring the health state of IDSs.

- Trust no node: an IDS can not suppose that any single node is fully secure (supposition: any node is not secure); because sensor nodes are compromising easily and disclosure information. Thus, in cooperative approaches, we have to attend that any nodes can not be fully trusted (supposition: any node is not reliable, completely).

⇨ Some of necessities are: error management, monitoring the health state of sensor nodes and security management.

- Be truly distributed: data gathering and analyzing them doing at some of specific location (calling cluster-heads).

⇨ Some of necessities are: loss of non-enforcing extra load to the special sensor nodes in the WSN, using detection mechanism, audit trial, warning dependence, distributed and collective response, accurate and comprehensive monitoring at the level of the entire network.

- Be secure: IDS must be robust and resistant against attackers' attacks and their activities [13, 15]. Compromising one or more sensor node 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: robustness and fault tolerant, error/fault 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 level) data communications and interactions;
- Scalability;
- Reaction and tracking capabilities;
- Ease of use and 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]; else, this kind of architecture threats the entire system security.
- Distributed approach: in this approach, it is possible to have one IDS per each cluster of nodes (CIDS); in this case, cluster-heads usually make decisions autonomously and independently; 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 appropriate 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 chained destruction.

⇨ The used 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 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 high level of the WSN architecture which has been installed and deployed on the powerful central server, called WSNIDS.

5. THE PROPOSED INTRUSION DETECTION ARCHITECTURE (IDA) FOR WIRELESS SENSOR NETWORKS

As Figure9 is showing, the suggestion architecture has a combinational (distributed and centralized) and hierarchical structure; thus, the proposed approach can be used in 1 or 2 levels of IDSs:

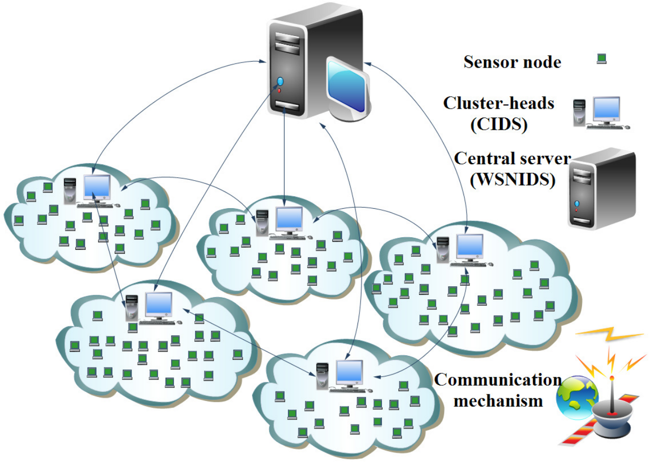


Figure 9. The proposed Intrusion Detection Architecture (IDA) for WSNs

5.1. Cluster-based Intrusion Detection System (CIDS)

CIDSs place on the low level of the proposed architecture (according to the Figure9); 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 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 special and limited preprocessing capabilities such as requirement data field extraction from the network packets and packets filtering. If an attack detects, according to the predefined action in policy and corresponding security rule, the IDS is responding to it.

In this level, decision making does in combinational; so, if the current traffic be from the internal of the cluster, the appropriate decision takes autonomously and independently; also, if the current traffic be from the boundary nodes (between different adjacent 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 estimation severity by current node) and will forward to the central server (centralized-cooperative decision making by CIDSs and WSNIDS).

- A cluster-head node, besides performing the common functions of typical sensor nodes like sensing and gathering information, routing packets into the WSN and forwarding data messages and retransmission, doing also intrusion detection functionalities.
- Some of common operations of each CIDS are: preprocessing, filtering, removing and/or 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 and minor information on the cluster-wide level; of course, it also using a distributed design for intrusion detection.
- In homogenous WSNs, CIDSs are same exactly on entire cluster-heads; they can broadcast, eavesdrop and listen to the messages (messages that come from other cluster-heads). 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, CIDSs are different from each others (since the systems and data types are different).

The main properties of CIDS are:

- Using local and minor information for intrusion detection (localize auditing);
- Producing very low false positive and false negative rates (due to existing complete and comprehensive Info-bases);

Each cluster-head in the WSN should has been a CIDS by following functionality (according to the Figure10):

- Cluster-based monitoring: each cluster-head monitors its immediate neighboring and nearby nodes (members of its associated cluster) to gather audit 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 cluster-heads to take appropriate decision, in collective.
- Action: each sensor node and cluster-head has responding mechanisms which allow it to react to the intrusion situations.

Internal components of the CIDS are (as shown in Figure10):

- 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;
- 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 evidence 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).
- Response module: once an intrusion occurred, node or compromised area will be detected and this module will does appropriate actions;

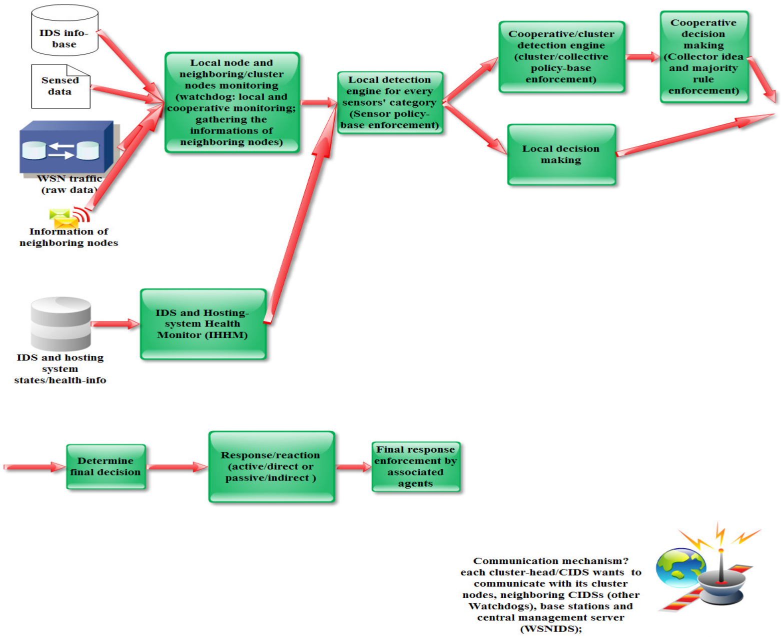

IDS info-base
Sensed data
WSN traffic (raw data)
Information of neighboring nodes
Local node and neighboring/cluster nodes monitoring (watchdog: local and cooperative monitoring; gathering the informations of neighboring nodes)
Local detection engine for every sensors' category (Sensor policy-base enforcement)
Cooperative/cluster detection engine (cluster/collective policy-base enforcement)
Cooperative decision making (Collector idea and majority rule enforcement)
Local decision making
IDS and hosting system states/health-info
IDS and Hosting-system Health Monitor (IHHM)
Determine final decision
Response/reaction (active/direct or passive/indirect)
Final response enforcement by associated agents
Communication mechanism? each cluster-head/CIDS wants to communicate with its cluster nodes, neighboring CIDSs (other Watchdogs), base stations and central management server (WSNIDS);

Figure 10. High-level architecture of the CIDS

5.2. Wireless Sensor Network wide level Intrusion Detection System (WSNIDS)

The WSNIDS place on the highest level of the proposed architecture; i.e. it installs and deploys on the heterogeneous central management server. As Figure11 shows, this system is a powerful and robust IDS which has some comprehensive Info-bases and mechanisms for intrusion detection, including a series of comprehensive and integrated policy-bases along with some agents to distinguishing anomalies. Also, the hosting system and deployment location of the WSNIDS is a powerful system which has high software and hardware facilitations, equipments and capabilities. Besides, the WSNIDS is managing existent systems (CIDSs) on the low level of the proposed architecture.

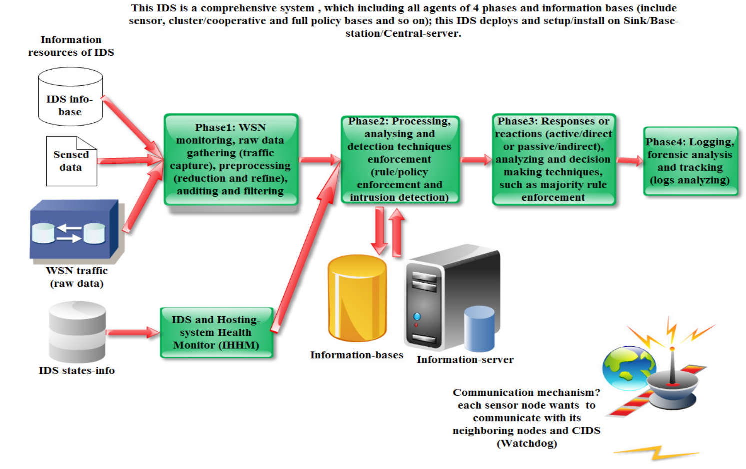

This IDS is a comprehensive system , which including all agents of 4 phases and information bases (include sensor, cluster/cooperative and full policy bases and so on); this IDS deploys and setup/install on Sink/Base-station/Central-server.
Information resources of IDS
IDS info-base
Sensed data
WSN traffic (raw data)
IDS states-info
Phase1: WSN monitoring, raw data gathering (traffic capture), preprocessing (reduction and refine), auditing and filtering
IDS and Hosting-system Health Monitor (IHHM)
Phase2: Processing, analysing and detection techniques enforcement (rule/policy enforcement and intrusion detection)
Phase3: Responses or reactions (active/direct or passive/indirect), analyzing and decision making techniques, such as majority rule enforcement
Phase4: Logging, forensic analysis and tracking (logs analyzing)
Information-bases
Information-server
Communication mechanism? each sensor node wants to communicate with its neighboring nodes and CIDS (Watchdog)

Figure 11. The basis architecture of the WSNIDS (intrusion detection procedures and main modules)

Figure11 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, tracking and forensic analysis (according to the Figure11 and Figure12).

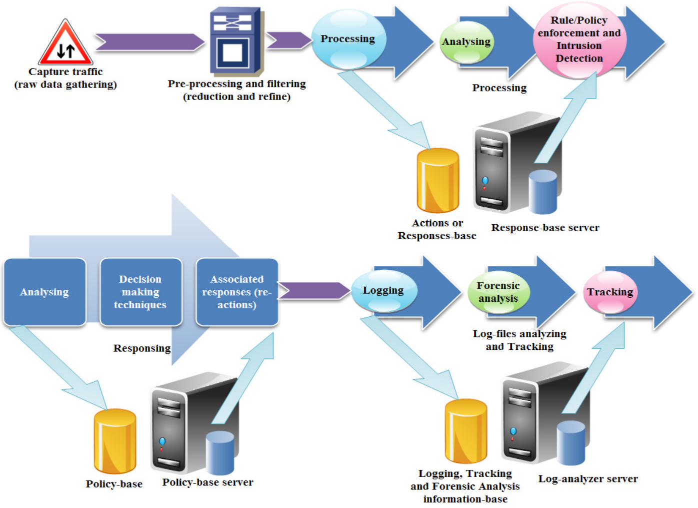

Capture traffic
(raw data gathering)
Pre-processing and filtering
(reduction and refine)
Processing
Analysing
Rule/Policy enforcement and Intrusion Detection
Processing
Actions or Responses-base
Response-base server
Analysing
Decision making techniques
Associated responses (re-actions)
Responsing
Policy-base
Policy-base server
Logging
Forensic analysis
Tracking
Log-files analyzing and Tracking
Logging, Tracking and Forensic Analysis information-base
Log-analyzer server

Figure 12. The WSNIDS work flow

Following figure (Figure13) is showing the data flow into the WSNIDS, in more detailed. As shown Figure11, Figure12 and Figure13, the WSNIDS is based on analyzing audited data messages, detected events by cluster-heads and inference the WSN's behaviors. 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.

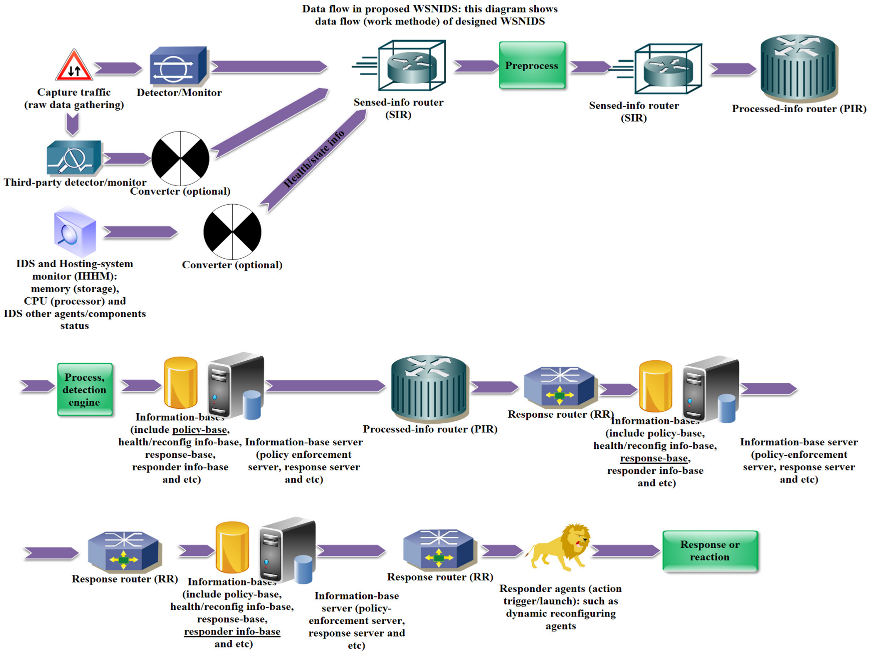

Data flow in proposed WSNIDS: this diagram shows data flow (work methode) of designed WSNIDS
Capture traffic
(raw data gathering)
Detector/Monitor
Sensed-info router (SIR)
Preprocess
Sensed-info router (SIR)
Processed-info router (PIR)
Third-party detector/monitor
Converter (optional)
Health/state info
IDS and Hosting-system monitor (IHHM): memory (storage), CPU (processor) and IDS other agents/components status
Converter (optional)
Process, detection engine
Information-bases (include policy-base, health/reconfig info-base, response-base, responder info-base and etc)
Information-base server (policy enforcement server, response server and etc)
Processed-info router (PIR)
Response router (RR)
Information-bases (include policy-base, health/reconfig info-base, response-base, responder info-base and etc)
Information-base server (policy-enforcement server, response server and etc)
Response router (RR)
Information-bases (include policy-base, health/reconfig info-base, response-base, responder info-base and etc)
Information-base server (policy-enforcement server, response server and etc)
Response router (RR)
Responder agents (action trigger/launch): such as dynamic reconfiguring agents
Response or reaction

Figure 13. The WSNIDS data flow

5.3. The major properties of the proposed architecture

The suggested system has following features:

- Distributed IDSs;
- 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;

- Independence and autonomous CIDSs (existing, operational and functional undependability); CIDSs are independent and autonomy; also, they do not have any dependency to each other, or they have minimum dependency; however, each CIDS does its functions independently, (until possible) almost entirely. It also takes decisions, alone.
- Ease of extensibility, too much scalability and high flexibility;
- Powerful detection process (since there are 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 WSN proposed architecture; for example, CIDSs to the WSNIDS, to establishing secure communications between different existent IDSs and preventing from intrusion of unauthorized systems (to this architecture);
- 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 depend on used routing protocol and response time (time consumed to search and finding appropriate pattern for query matching into the Info-bases);
- Fault tolerant and dynamic reconfiguration:
  - Using backup network equipments, such as nodes in low level and medium level of proposed architecture; i.e. there are some backup sensor nodes and backup cluster-heads;
  - Using backup agents into the IDSs;
  - Clusters overlapping (increased stability);
  - Predicting the location deployment of sensor nodes and other backup network components and equipments in the WSN;
  - Existing dynamic reconfiguration agents for itself CIDS, WSNIDS and other network equipments;
  - Updating resources and Info-bases in manual or automatic; for example, by using new patterns of (new) 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:
  - Itself IDS protection (monitoring the health state of IDSs and their hosting systems, continuously) and stability of deployment hosting system of IDSs;
  - The architecture is dependence to the data flow (network traffic);
  - Logging;
  - Using cryptography and secret key to exchange information between sensor nodes and cluster-heads, and between cluster-heads and central server (WSNIDS);

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 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, special and high-level properties and finally, the properties of the selected routing protocol. 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. Category1: Preprocessing, processing, assessing and managing properties

As Table1 is showing, the proposed architecture supports different dimensions of IDSs' processing properties. For example, the IDA's monitoring level is almost 96 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 82.7 percent. Besides, the IDA has dynamic re-configurability capability about 66.9 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 about 81.87 percent, in average.

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	-----		96
2	Extendibility and flexibility	-----		82.7
3	Dynamic re-configurability capability	-----		66.9
4	Local and remote control capabilities	Yes		-----
5	Distributed databases capabilities	Yes		-----
	Average (percentage)	**-----**		**81.87**

6.2. Category2: Operational properties

Table2 is representing the different aspects of the IDA's operational requirements. According to the following table, the IDA supports real-time detection property almost 80.6 percent. Also, it has the content-based (body of a packet) detection and context-based (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 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 75.23 percent, in total.

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	-----		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	Hierarchical reporting structure	Yes		-----
6	Automatic reaction to the intrusions	Yes		-----
	Average (percentage)	**-----**		**75.23**

6.3. Category3: Output requirements

Following table (Table3) 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.

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)	**-----**		**-----**

6.4. Category4: Technical requirements

Table4 is representing and questioning the IDA's technical properties. For example, ease of implementation of the proposed system is evaluated about 85 percent; the IDA has fault tolerant, scalability and robustness capabilities, each one almost 74, 92.5 and 64.2 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 78.48 percent, in average.

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	-----		85
2	Fault tolerant capability	-----		74
3	Scalability	-----		92.5
4	Robustness	-----		64.2
5	Safety (against unauthorized access)	-----		76.7
6	Possibility of using key management and authentication mechanisms	Yes		-----
7	Enforcing extra load to the WSN	No		-----
	Average (percentage)	**-----**		**78.48**

6.5. Category5: Special and high-level properties of the IDA

Following table (Table5) 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 from each others. 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. CIDSs can operate by using partial and local auditing data, in cluster-level. 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 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 taking and using distributed approach). The proposed system is a secure architecture; i.e. it is resistant and robustness against attacks; so, if 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 percent. This system can detect chaining attacks by using powerful detection process and audit trial mechanisms (about 64.8 percent). The IDA is evaluated as an optimal system in energy consumption; since, it is attending to the energy consumption in designing step (almost 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 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 data flow (network traffic); its dependability is evaluated almost 87.5 percent. The suggested architecture is consistent to the centralized and autonomous operations in different levels of WSNs; its consistency is evaluated about 88.2 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 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 85.5 percent. It is also possible to update the IDSs (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 CIDSs) and if necessary, taking cooperative decisions (by CIDSs, collector and the central server). As a result, the IDA is included different properties of this IDSs' requirement category almost 80.86 percent, in total.

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	-----		78.6
3	Centralized management on the WSN	Yes		-----
4	Localize auditing capability	-----		92.5
5	Minimize resources property	-----		66.3
6	Accurate management of resources and monitoring the health state of IDSs and the WSN components	Yes		-----
7	Truly distributed	-----		81.8
8	The IDA security	-----		67.5
9	Centralized control on inter-components data communications	Yes		-----
10	Interaction level between different network components	-----		93
11	Ability to detecting chaining attacks	-----		64.8
12	Attending to the energy consumption	-----		75.6
13	Strength of detection process	-----		89
14	Possibility to taking back-up designs	Yes		-----
15	Data flow dependability	-----		87.5
16	Consistency to the centralized and autonomous operations of the WSN	-----		88.2
17	Existing different control locations	Yes		-----
18	Ease of updating	-----		85.5
19	Possibility to updating the IDSs (CIDSs and the WSNIDS) and operational using of them, simultaneously	Yes		-----
20	Combinational decision making technique	Yes		-----
	Average (percentage)			**80.86**

6.6. Category6: Properties of the selected routing protocol

Following table (Table6) is presenting and discussing different characteristics of the selected routing protocol (LEACH); also, it is showing the evaluated average value which they have been concluded from analyzing and assessing questionnaires. As Table6 shows, the selected routing protocol consistent to the proposed model, about 74.5 percent. It is also consistent to the operating environment and variable configuration of the WSN (i.e. its dynamic topology, heterogeneous and mobile properties), almost 86.9 percent. The selected routing protocol is optimal about energy consumption; because it supports operations such as data aggregation. The selected routing protocol is scalable and fault tolerant, about 95 and 77.2 percent (in order). This protocol is attending to the QoS criteria such as energy consumption and finding optimal routes. The selected routing protocol is fairness protocol; because it is distributing energy consumption between different nodes into the WSN and it does not use or impose pressure on an/some especial nodes. Finally, the selected routing protocol is supporting the different properties of this IDSs' requirement category about 83.4 percent.

Table 6. Properties of the selected routing protocol

No.	**Question**	**Functional properties**		**Non-Functional properties**
		Yes	**No**	**In percentage (0 - 100) : Total average**
1	Consistency with the IDA	-----		74.5
2	Consistency with the WSN	-----		86.9
3	Optimality on energy consumption	Yes		-----
4	Scalability	-----		95
5	Fault tolerant	-----		77.2
6	Attention to the QoS criteria	Yes		-----
7	Fairness	Yes		-----
	Average (percentage)	**-----**		**83.4**

7. CONCLUSION

The purpose of this paper is considering intrusion detection problem on WSNs and designing an Intrusion Detection Architecture (IDA) for these networks, of course by attending to their restrictions. The suggested system depends on situations, the WSN's application domain, the requirement security level and other things such as its cost, can be used and implemented in 1 or 2 levels; including: CIDSs (surveillance, monitoring and control in cluster-level) on cluster-heads and the WSNIDS (monitoring and control in the WSN-wide level or level of the entire WSN) on the central management system. The main properties of the suggested architectures are as following:

- The IDA: hierarchical, distributed, scalable and clustering;
  - Distributed systems are more scalable and more robust;
- The proposed IDSs (CIDS and 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;
- Detection method:
  - Combinational (specification-based);
  - Uncentralized (detection in 1 or 2 levels); because these networks are application-oriented;
- Decision making approach: combinational;
  - About each cluster's nodes, the corresponding CIDS makes decision, independently and autonomously;
  - About anomaly occurrence or boundary nodes, associated 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, 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, cluster-head is very near to attacker (one-hop distance);
- 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;
- Centralized on routing layer, mainly;
- Using a hierarchical routing protocol;
- According to the Table1, Table2, Table4, Table5 and Table6, following table (Table7) is representing integrated average values of different IDSs' requirement classes.

Table 7. Total average value of different properties category

No.	Properties class	Total average value (in percentage)
1	Preprocessing, processing, assessing and managing properties	81.87
2	Operational properties	75.23
3	Technical properties	78.48
4	Special and high-level properties	80.86
5	Properties of the selected routing protocol	83.40
	Average value (in percentage)	**80.92**

- According to the Table7, following figure (Figure14) is formed. Figure1 is showing the sum average values of different IDSs' properties categories; in other words, the IDA supports different categories of IDSs' required properties (as Figure14 shows).

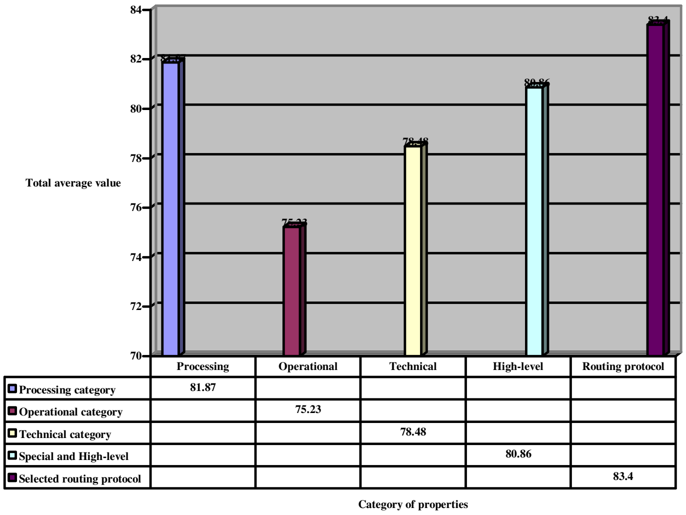


Figure 14. The sum average values of different IDSs' properties categories

- 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 IDA 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. The suggested routing protocol has different properties, which they are proper to the WSN area; it is evaluated that the selected routing protocol supports different required properties of the IDA and the WSN, about 83.40 percent, in average; i.e. it is proper to the IDA and the WSN, almost 83.40 percent. As a result, the proposed system is included different IDSs' requirement categories almost 80.92 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 cluster and cluster-head; i.e. it can uses from the local cluster-wide information to detects intrusions (it does not need to any another information: CIDS). Also, if necessary, sensor nodes, cluster-heads and WSNIDS 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 collector and if necessary, with WSNIDS, to detect and make final decision on detected anomaly. It is hoped to this research able us to 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 mechanism;
- Providing higher level of security, fault tolerant and robustness for suggested architecture;
- Centralizing and providing more detailed information about system activities for forensic analysis;
- Data efficient management and providing fast query methods;
- Developing user friendly interfaces which allow dynamic reconfiguration of systems (the CIDSs and the WSNIDS) and representing the activities of these systems, in graphical;
- Methods for minimal and optimization energy consumption and network delay in hierarchical routing protocols;
- Techniques for using of mobile nodes and routing in these such WSNs;

Work in this area is growth, always in continuous 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.

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 (JIAS); ISSN 1554-1010 Volume 6, pp. 195-215; 2011.

[2] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy; A Comparison of Link Layer Attacks on Wireless Sensor Networks; Journal of Information Security (JIS); 2011.

[3] K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, SMIT, Sikkim, India; 2010.

[4] T. A. Zia; A Security Framework for Wireless Sensor Networks; Doctor of Philosophy Thesis; The School of Information Technologies, University of Sydney; Feb 2008.

[5] M. Saxena; Security in Wireless Sensor Networks: A Layer-based Classification; Department of Computer Science, Purdue University.

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

[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; Skopje, Republic of Macedonia.

[8] J. Yick, B. Mukherjee and D. Ghosal; Wireless Sensor Network Survey; Elsevier's Computer Networks Journal 52 (2292-2330); Department of Computer Science, University of California; 2008.

[9] C. Karlof and D. Wagner; Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures; Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols; In First IEEE International Workshop on Sensor Network Protocols and Applications; University of California at Berkeley, Berkeley, USA; 2003.

[10] A. Perrig, R. Szewczyk, V. Wen, D. culler and D. Tygar; SPINS: Security Protocols for Sensor Networks; Wireless Networking ACM CCS; 2003.

[11] B. Krishnamachari, D. Estrin, and S. Wicker; The Impact of Data Aggregation in Wireless Sensor Networks; International Workshop on Distributed Event-Based Systems, (DEBS '02), p 457-458; 2002.

[12] V. Handziski, A. K¨opke, H Karl, C. Frank, and W. Drytkiewicz; Improving The Energy Efficiency of Directed Diffusion Using Passive Clustering; in Proc. 1st European Workshop on Wireless Sensor Networks, pp. 172 – 187, Berlin, Germany; 2004.

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

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

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

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

[17] J. Molina and M. Cukier; Evaluating Attack Resiliency for Host Intrusion Detection Systems; Information Assurance and Security Journal; 2009.

[18] 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.

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

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

[21] S. Zanero and S. M. Savaresi; Unsupervised Learning Techniques for an Intrusion Detection System; ACM Symposium on Applied Computing; 2004.

[22] O. Depren, M. Topallar, E. narim and M. K. Ciliz; An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks; 2005.

[23] R. A. Kemmerer and G. Vigna; Intrusion Detection: A Brief History and Overview; 2002.

AUTHOR BIOGRAPHY

H. Jadidoleslamy is a Master of Science student at the Guilan University in Iran. He received his Engineering Degree in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Iran, in September 2009. He will receive his Master of Science degree from the University of Guilan, Rasht, Iran, in March 2011. His research interests include Computer Networks (especially Wireless Sensor Network), Information Security, and E-Commerce. He may be reached at tanha.hossein@gmail.com.