A Lightweight Intrusion Detection System Based on Specifications to Improve Security in Wireless Sensor Networks

M. Sadeghizadeh, O. R. Marouzi
Faculty of Computer and IT Engineering, Shahrood University of Technology, Shahrood, Iran
Faculty of Electrical and Robotic Engineering, Shahrood University of Technology, Shahrood, Iran
Emails: m.sadeghizadeh@shahroodut.ac.ir, marouzi@shahroodut.ac.ir
Corresponding author: M. Sadeghizadeh

***Abstract*- Due to the prevalence of Wireless Sensor Networks (WSNs) in the many mission-critical applications such as military areas, security has been considered as one of the essential parameters in Quality of Service (QoS), and Intrusion Detection System (IDS) is considered as a fundamental requirement for security in these networks. This paper presents a lightweight Intrusion Detection System to protect the WSNs against the most important of routing attacks in network layer based on their extracted specifications. The proposed IDS, in contrast to related works that often focuses on a specific attack, covers almost all recognized important routing attacks in WSNs. With the full simulation of the routing attacks and the careful examination of their behavior, we extracted key specifications to identify them in the proposed system. Also, due to local operations provided to detect and significantly reduce communications, the proposed method is a lightweight approach. Another advantage of the proposed method is reducing false alarms rate by applying appropriate thresholds. We considered all performance criteria to evaluate and compare the proposed method. Simulation results show that the proposed system is an effective and lightweight IDS in WSNs due to high detection accuracy, low false alarms rate, and low power consumption.**

***Index Terms*-** Wireless Sensor Networks (WSNs), Routing Attacks, Intrusion Detection Systems (IDSs), Specification Based Detection.

I. INTRODUCTION

Recent advances in electronics and wireless communications have made it possible to create sensor nodes with low energy consumption, small size, reasonable prices and various applications. The WSNs are made up of a large number of small nodes that have capabilities such as sensing, processing, and communication to monitor real events in diverse environments. These highly

Manuscript received 15-April-2018 and revised 8-June-2018,
Accepted on 27-August-2018
P- ISSN: 2322-4088
E- ISSN: 2322-3936

desirable and cost-effective networks play different roles in a wide range of applications, such as military surveillance, fire control, and safety monitoring of buildings. However, resource constrains, such as limited processing power, memory and energy are main challenge in WSN design and application [1].

Given that WSNs are often used in remote and unprotected locations or where adverse operating conditions or even hostile operating conditions, they are highly susceptible to intrusions and security attacks [2]. Most of attacks try to cause a sharp decline in network performance using this weakness. Therefore, security in WSNs has become an important issue, especially if these networks are involved in critical processes. Secure WSNs have critical importance in the military (tactical) applications, so that a security gap in the network can weaken its own forces on the battlefield [3].

A series of attacks that are common in WSNs and severely degrade network performance are network layer and routing attacks. In this paper, a lightweight IDS based on the characteristics of attacks is proposed to protect the WSN against the most important routing attacks. In the proposed method, based on the analysis of the behavior of network layer attacks and their characteristics, detection operations are performed without any communication, which reduces energy consumption in nodes. In addition to a significant energy saving of our method, its appropriate detection rate along with low false alarm rates, suggests this as a desirable IDS for WSNs. In order to validate the proposed IDS in simulations, all performance criteria have been evaluated.

This paper is organized as follows: In Section II, we introduce the common security attacks in WSNs, then the IDSs are described and, finally, the most important related works are presented. Section III describes the proposed IDS. In Section IV, we will simulate the proposed IDS and present the related results. Finally, the paper ends with a conclusion and future works.

II. PRELIMINARIES

In this section, common attacks in WSNs are introduced, and then IDSs are described along with their requirements. Finally, a review on the most important IDSs devised for WSNs is presented along with the introduction of their advantages and shortcomings.

A. Common Attacks in WSNs

Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable and susceptible to numerous security attacks that can adversely affect their proper functioning and challenge the security of them [2]. The most important attacks in WSNs are network layer and routing attacks [2]-[6]. In the following, network layer and routing attacks are described:

***Sinkhole Attack* —** In this attack, the attacker node acts so that for their neighbors in cases such as routing parameters seem attractive or as a base station. Therefore, neighboring nodes chose the malicious node as the next node in their data routing. In this way, as shown in Fig. 1, this attack

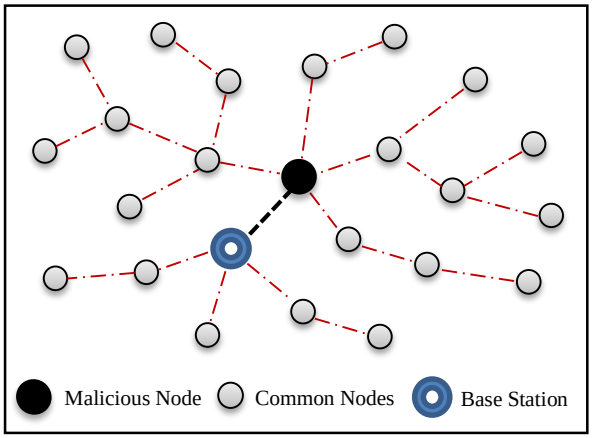

Fig. 1. Sinkhole attack through a false sink [7].

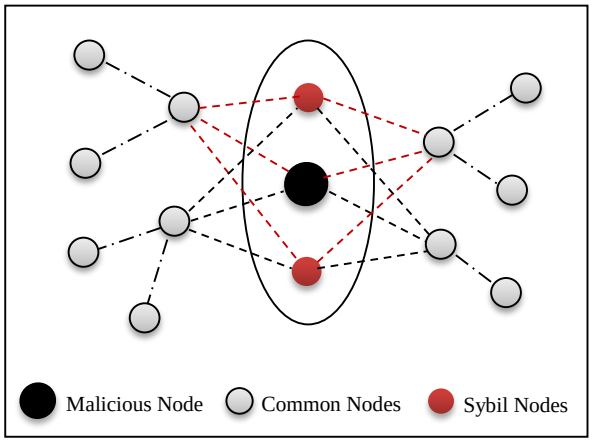

Fig. 2. Sybil attack through several fake paths [8].

creates a false sink and exploits network communications without authentication, As a result, the information don't reach the base station and network services are damaged [7].

Sybil Attack — In a Sybil attack a malicious node illegally in different ways taking on multiple identities in the WSN. The malicious node together with all the identifiers under its control (includes multiple nodes) are called Sybil nodes. This attack disrupts the performance of routing algorithms, distributed storage, voting, and fair resource allocation through identifiers. For instance, as shown in Fig. 2, a malicious node generates multiple paths with the help of the Sybil identifiers and disrupts the operation of the routing protocol [8].

Hello Flood Attack — A malicious node uses hello messages to convince sensor nodes and trap them in WSNs. In this attack, the adversary that is a relatively strong node sends hello packets with a high-powered transmitter to a number of sensor nodes in a wide area of WSN. In this way, sensors are convinced that the adversary is their neighbor. So victim nodes try to work with the adversary when sending data to the base station, and eventually eliminated due to excessive consumption of energy to futile sending of data [9].

Selective Forwarding Attack — Multihop sensor networks operate on this assumption that the intermediate nodes on the route will accurately forward packets to the next node. In this attack, the adversary may prevent forwarding some packets to the next node and drop them to ensure they are not distributed on the network. A specific form of this attack is that the adversary acts as a black hole and drops all packets [10].

Denial of Service Attack (DoS) — In this attack, the malicious node, which is usually a high-power node, by sending a flood of messages to the target node, does not allow to serve other nodes in the network, and thus the cluster operation is completely disrupted. Occasionally, this attack may even disrupt the entire network by the attack to several important nodes on the network [11].

B. Intrusion Detection Systems

In general, any type of unauthorized or unwanted activity in a network is called intrusion. An IDS is a set of tools, methods, and resources to help identify, assess, and report intrusions. IDS is not a single, separate unit, but rather part of an overall protection system that is installed alongside a network node. Intrusion is defined as any set of activities that attempt to endanger the integrity, confidentiality or availability of a resource, and Intrusion Prevention System (IPS) includes methods such as encryption, authentication, access control, secure routing, etc. is considered as the first line of defense against intrusions [12].

However, it should be noted that in any secure or less secure network, it cannot be completely prevented from intrusions. When attacking to a network and intrusion to it, some nodes are captured by the attacker and thus malicious node can identify and reveal their confidential information such as security keys. This will lead to the failure of the intrusion prevention operation and Jeopardize network security. In such a situation, the existence of an IDS in the network by timely detecting of intrusions can prevent the disclosure of security information and the waste of resources. Therefore, after IPSs, IDSs are considered as the second line of defense against attacks and intrusions. The expected operating conditions in IDS will be as follows [13], [14]:

- Not add new flaws and weaknesses to the network.
- Less use of network resources, and not reducing network performance by imposing overhead.
- Low False alarm rate, which is equivalent to the percentage of normal activity that is detected as anomaly.
- High detection rate, which is equivalent to the percentage of anomalies that have been properly detected.
- Run continuously and act impalpable for the system and users (Transparency principle).
- Should be in accordance with standards to allow for future cooperation and development.

Each IDS has three main components [14], [15]:

- ***Monitoring Section:*** This section is used to monitor local events and neighbors and often by traffic analysis and local events, controls the resources efficiency.
- ***Analysis and Detection:*** This module is the main part of the IDS, which is dependent on the modeling algorithm. In this section, the behavior and activities of the network are analyzed and decided to declare them as an intrusion.
- ***Warning section:*** This section is responsible for reaction against intrusion, which generates an alarm about the detection of an intrusion.

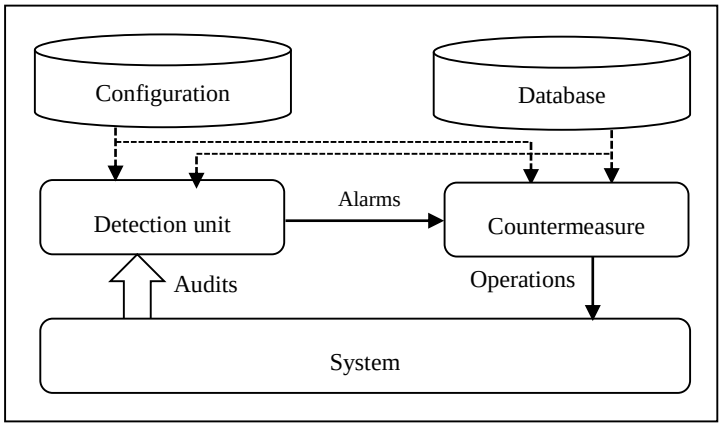

Fig. 3. Diagram of a basic Intrusion Detection System [13]

Fig. 3 presents a diagram of a basic IDS [13]. As shown in Fig. 3, there are three inputs for detecting intrusion: a database of known attacks, the current configuration of the system, and audit information that describes events occurring in the system.

When all necessary information are sent to the detection unit, it determines what information is important and performs appropriate actions to detection the intrusions.

III. Related Works

So far, many IDSs have been introduced for WSNs, often focused on a specific attack, as [7]-[11]. There are also a few of IDSs that can be used on a number or all of the available attacks, which we will discuss in the following, the most important ones.

In [16], a hierarchical architecture for IDS along with hierarchical data processing is proposed. They provided a two-level clustering, which at first-level, cluster-heads would manage the clusters, and at the second level, cluster-heads would communicate with the gates and connect to the base station through them. They have focused on the concept of single-hop clustering in all of their proposed architectural experiments. The main reason for their focus on single-hop clustering is that the highest detection rate is when the nodes are connected in a single-hop relationship with the cluster-head, and as the number of jumps increases, the detection rate will also decrease linearly. The fundamental problem of their hierarchical architecture for security in WSNs is that it will only be used for industrial applications.

In [17], an IDS is proposed based on the clustering method. The proposed method also provides security for the cluster-heads. In their way, cluster members monitor the cluster-head in a timely manner. With this method, all members of the cluster will be saved in energy consumption. In contrast, cluster members are monitored not by cooperation between cluster members but by cluster-heads, which saves more energy in cluster members. According to the results, they showed that their IDS is much more efficient than the other available systems. The main problem in proposed method is

the key management mechanism. This mechanism helps to establish pairwise keys relationship in the between nodes and assumes that the nodes are fixed (non-mobile), and is not possible to add new nodes to the network after the pairs keys are fixed. Given that WSNs periodically require the release of new nodes, this creates a flaw in their model.

In [18], authors proposed lightweight methods for detecting abnormalities in WSNs. Their main idea is to reuse existing system information (such as neighboring list, routing tables, active and deactivated schedules, received signal strength information, MAC layer scheduling) that produced in different layers of the network protocol stack in the OSI model, in particular in the physical, MAC and routing layers. In order to provide a better detection rate, the authors suggested that multiple detectors should be monitored for different layers of the OSI model. This is not possible for sensor networks, since monitoring the intrusion of different layers and coordinating between these observers can quickly consume limited resources in WSN. On the other hand, the authors proposed their plans only for external attacks and did not consider internal attacks. This selection is not enough because nodes in a WSN are very susceptible to internal attacks (physical capture attack, Sybil attack, etc.).

In [19], a lightweight ontology-based wireless IDS (OWIDS) has been introduced that uses a series of guard nodes to detect intrusions. The guard node is, in fact, a sensor node that knows how to detect attacks. These nodes monitor the sensor nodes by collecting information from the sensor nodes and apply detection knowledge on them. In this method, in order to increase the strength of the guard nodes in detecting attacks, the relationships between sensor nodes are also defined in detection knowledge. The proposed method is lightweight in energy consumption, but it will increase network cost due to the use of guard nodes, which is an overhead for the network. Also, the detection accuracy depends on the number of guard nodes in the network.

In [20], in order to detect sinkhole and selective forward attacks in cluster-based WSNs, proposed a centralized IDS based on the misuse detection that, by defining more rules, provides an extension of the proposed method in [21]. The main idea of their method, which uses a centralized detection technique, is to collect the control packets from the cluster-heads at the base station and apply the misuse detection rules on all data, And the final decision making to detect attacks. The main problem with their method is that it is only capable of detecting black-hole and selective forward attacks and cannot detect other attacks.

In [22], a Global Hybrid IDS (GHIDS) has been proposed that to achieve the goal of high detection rates and low false alarms, used combination of a technique based on support vector machine (SVM) for detecting anomalies, with a set of signature-based detection rules to identify attacks in cluster-based WSNs. The results of the simulations show that the proposed method is in a desirable condition In terms of the detection rate and the false alarm rate. But the underlying problem is the high energy consumption due to the use of an anomaly detection technique based on SVM, which is somewhat inappropriate for the sensor network.

In [23], a Knowledge-Based intrusion Detection Strategy (KBIDS) is proposed to detect several types of attacks under different network structures, that aims to create a stand-alone detection model from network structure for WSNs. Their proposed mechanism is based on the fact that various types of attacks are very likely to have various forms of density in the feature space. They collected the network traffic and used it as the characteristics of the behavior of random networks in the feature space. Then the density forms can be considered as an indicator for detecting normal and abnormal network behavior. The simulation results of the proposed method in [23] on the sinkhole, hello flooding and DoS attacks indicate the proper detection accuracy and high compatibility with the network structure than the existing works.

In [24], a hybrid IDS is proposed for cluster-based WSNs that detect malicious nodes by integrating misuse detection rules and functional reputation. The main idea of the proposed method is that instead of detecting attacks only at nodes level, they propose a collaborative and centralized design using the mutual trust assessment between all network components, in which each sensor node computes functional reputation values for its neighbors by observing their activities (transmissions and data aggregation). In order to achieve this, they have defined five functional reputation metrics and benefit from the high detection rate of the misuse detection method by applying the relevant rules. The main problem with their methodology is that only have expressed their energy consumption results and have not presented any discussion of the detectable types of attacks and their detection rates.

In [25], a multi-class method is proposed based on Error Correcting Output Codes (ECOC) algorithm in order to get better performance of attack recognition in WSNs. This method can be used to classify the traffic data collected by network nodes to determine whether the system is invaded by attackers. Aiming to enhance the accuracy of attack detection, the multi-class method is constructed with Hadamard matrix and two-class SVM. Also In order to minimize the complexity of its algorithm, sparse coding method is applied.

In [26], a hybrid IDS for WSNs is proposed that exploits advantage of support vector machine (SVM) for detecting anomalies and signature model to identify attacks in cluster-based WSNs and provide a global lightweight IDS. The results of the simulations show that the proposed method is in a desirable condition In terms of the detection rate and the false alarm rate. But the underlying problem is the high energy consumption due to the use of an anomaly detection technique based on SVM.

IV. PROPOSED INTRUSION DETECTION SYSTEM

So far, various methods have been proposed to detect intrusion in WSNs. But the main challenge in existing methods is still high energy consumption and the lack of coverage of most attacks. In this section, we want to detect the most important routing attacks on these networks effectively by providing a lightweight IDS.

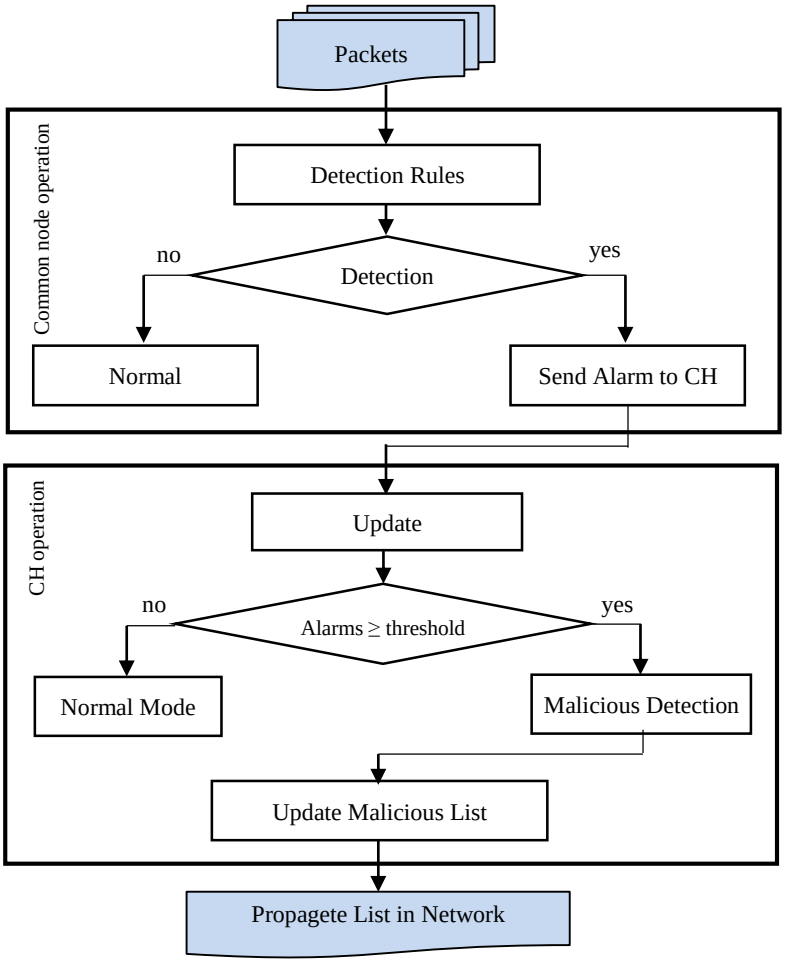

Fig. 4. Operations of proposed intrusion detection system

We use a specification-based intrusion detection that can keep network performance to the desired level due to the speed of its operation, the reduction of energy consumption and the low error rate in detection. We also used node clustering technique in the proposed system to take its advantages in intrusion detection process at the network.

Clustering of nodes is an energy efficient approach for WSN. In clustering, Instead of sending data directly to BS, nodes send data to their corresponding CH via multiple hop communication and CH sends aggregated data to BS. So clustering avoids long distance communication of nodes to BS and is preserving energy of sensor nodes [27].

In general, based on the capabilities of network nodes, there are two methods for clustering nodes in WSNs [28], [29]:

1. Static clustering: In this type, CHs have more capabilities than common nodes and are manually placed in the environment. Then the common nodes are allocated to the closest cluster based on the distance from the cluster heads. In reference [30], this method is used for clustering.
2. Dynamic clustering: In this type of clustering, usually all nodes have similar capabilities. Since the operation of CHs results in more energy dissipation, CHs change periodically due to the

load balancing and the longer lifetime of the network. An example of this method has been used in [27] and [31]. LEACH (Low Energy Adaptive Clustering Hierarchy) [32] is the most popular and attractive dynamic clustering algorithm which is widely used for its simplicity.

We used both the static and dynamic clustering in our simulations for the proposed method.

The proposed method, presented in Fig. 4, is organized at two levels of the common nodes (first level) and cluster-head nodes (second level). At the first level, first, the normal nodes test the rules for detecting the various attacks (which are extracted from the characteristics of each type of attack), and if existing any anomalies referring it to the cluster-head for further investigation. This specification that presented in Section II.A is given based on the analysis of the behavior of the attacks and their operation.

At the second level, cluster-heads will check the received alarms from different nodes and, if they exceed the threshold, are detected as an attack, and the list of malicious nodes is updated and sent to all cluster nodes.

A. Detection rules based on the specifications

In this section, based on the analysis of the behavior of various attacks and specifications extracted from them, we will describe the rules of their detection.

Detection of Denial-of-Service Attack: In this attack, the malicious node, considering the high speed of sending packets to other nodes, intends to increase their workload to the extent that they lose their usual service. Therefore, an attacker can be identified by checking the interval between received packets (IRP). Additionally, in most cases, the attacker sends packets with high power, which can be identified by the Received Signal Strength Indicator (RSSI).

For determination of RSSI threshold, assume that a node sends a radio signal at power P_0. The amount of RSSI received in node *i* will be as follows [33]:

$$R_i = P_0 . K \,/\, {d_i}^{\alpha} \tag{1}$$

Where d_i is the Euclidean distance from the node *i* to the assumed node, α is the distance-power gradient and for free space is considered to 2, and *K* is a constant obtained from equation (2):

$$K = Gt . Gr . (\frac{\lambda}{4\pi})^2 \tag{2}$$

$$R_i = P_0 . Gt . Gr . (\frac{\lambda}{4\pi})^2 \,/\, {d_i}^2 \tag{3}$$

Where *Gt* is the antenna gain in the transmitter, *Gr* is the antenna gain in the receiver, and λ is the wavelength, which according to IEEE 802.11 standard their values are *Gt*=1.0, *Gr*=1.0 and λ=0.125. In equation (3), the RSSI is determined by the fact that P_0 is the same in the network nodes.

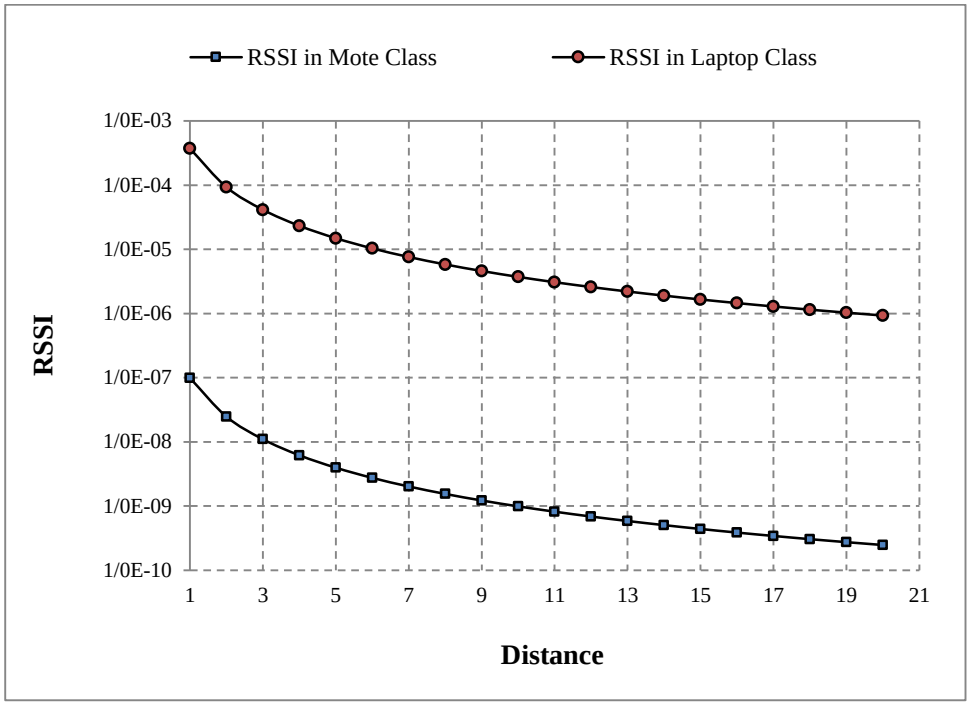

Fig. 5. RSSI as a function of the changing node distances.

In Fig. 5, the changes in the received RSSI as a function of the changing distances between network nodes (based on node density), for both classes of common nodes (mote class) and powerful nodes (laptop class) depicted.

According to the significant difference in RSSI between these two classes of nodes, it's easy to set the threshold value for the RSSI received in the common nodes. This threshold value is presented based on the simulated network parameters in Table 3.

To determine the IRP threshold, since that in a DoS attack, the malicious node must send packets to target nodes at a very high speed to prevent them from serving on the network, so there is a significant difference in IRP between normal mode and the DoS attack in network. Of course, depending on the type of network and the average time interval between the packets in them (Between a fraction of seconds to several minutes), in each application, this parameter should be set at the beginning of the network operation.

Detection of Hello flood attack: Because in a Hello flood attack, in most cases an attacker is a high-power external node, we can detect it via the received RSSI. Also, given that this attack causes an increase in routing overhead (see Fig. 15), we can also detect it via the rule of the time interval between routing messages (IRM). In order to determine the upper bound of IRM, according to the significant difference between the routing overhead in this attack and other attacks, with the same mechanism as the IRP threshold determination, we set the IRM threshold value based on the simulated network parameters.

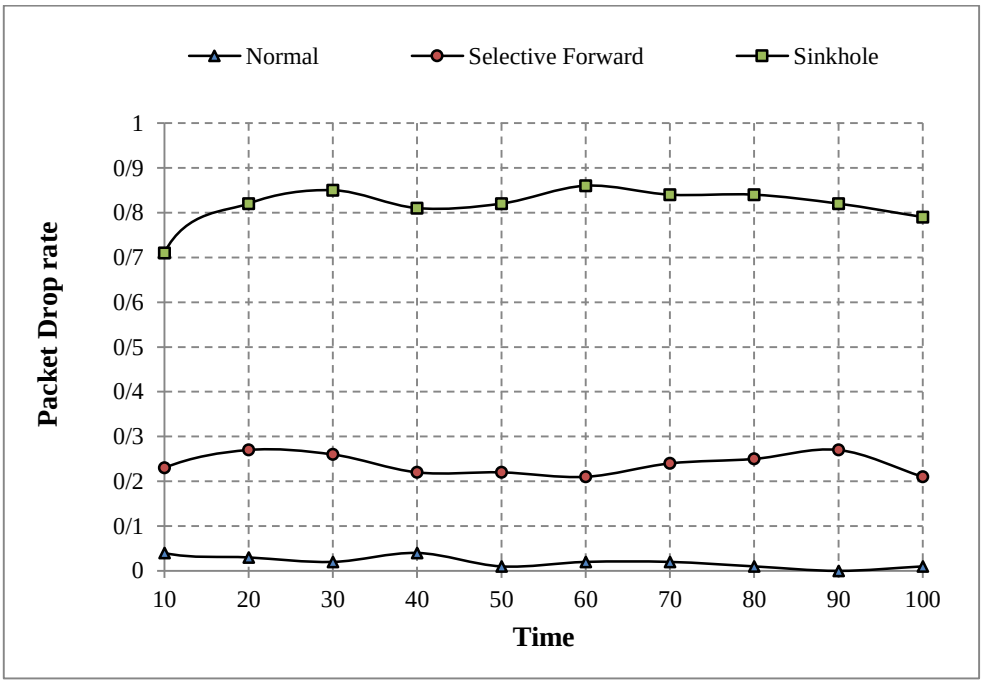

Fig. 6. Packet Drop Rate as a function of the changing Time.

Detection of Sinkhole attack: The most important parameter in detecting a sinkhole attack is a rise in the packet drop rate, which common nodes can detect it through an overhearing operation. Thus, if the packet drop rate is higher than the usual rate, an alarm will be generated and sent to the cluster-head. Relationship (4) shows how to calculate the packet drop rate by overhearing.

$$PacketDrop\ Rate = 1 - \frac{packets\ actualy\ forwarded}{packets\ to\ be\ forwarded} \quad (4)$$

According to (4) and comparison with the threshold, it is possible to detect those attacks that based on the packet loss, especially the sinkhole and wormhole attack. The relationship (5) shows the range of PDR changes. The result closer to one shows a stronger attack.

$$0 < Threshold_{PDR} < PDR < 1 \quad (5)$$

In this type of attack, in addition to the above criteria, the attacker can also be identified according to the received RSSI.

Detection of Select Forwarding attack: Given the fact that the basis of these attacks is also the removal of packets, such as a sinkhole attack can use overhearing method and detect the attacker by calculating packet drop rates. Of course, according to the type of operation, the packet drop rate in these attacks varies and is generally lower than the sinkhole attack. So the threshold for PDR should be lower. In order to determine the thresholds for packet drop rates in sinkhole and selective forward attacks, the chart of the packet drop rate in three different modes is plotted in Fig. 6. As can be seen, the drop rate in the sinkhole attack is very high, the average of about 0.84, and in the selective

forward attack, it is about 0.26, while in normal mode, this rate is below 0.02. Thus, according to Fig. 6, it is easy to determine the thresholds for packet drop rate for sinkhole and selective forward attacks, which are presented in Table 3.

Detection of Sybil attack: The most important feature that can be used to identify a Sybil attack is that all nodes with different identifiers are in the same place as the network since they all are under the control of a malicious node with a unique hardware. Due to the heavy calculations related to the localization of nodes in the network, we can only detect the attack by storing and comparing the received signal strength indicator (RSSI) for received messages. The method is that if a node is suspected to Sybil attack on *Si* and *Sj* nodes, it is sufficient to calculate the RSSI ratio for them and send it to the cluster-head to give it the final decision. In the cluster-head, if several alert messages are reported with the same RSSI ratio, those suspicious nodes (the *Si* and *Sj* nodes) will be known as a Sybil attack.

Cluster-head operation and final decision making: Whenever an alert message is sent to the cluster-head about a malicious node from other nodes, the cluster-head will make the final decision by updating the alert status and comparing it to the threshold. As shown in Algorithm I, if the alerts exceed the threshold, the assumed node is identified as a malicious and placed in the malicious list and then updates the malicious list of other nodes in the cluster by sending messages to them.

In order to determine the $threshold_{Alarm}$ for detecting attacks in the cluster head, the degree of neighborhood for the nodes in a WSN must be determined, which is done at the beginning of the network. Therefore, in order to detect an attack, it is enough that at least half the neighboring nodes send an alarm message to the CH. This threshold value is presented based on the simulated network parameters in Table 3.

```
Receive (alert);
 If (Looking (alert, intrusion alert))
 {
     Attacker_Count [Node-ID] ++;
     If (Attacker_Count [Node-ID] >  Threshold_Alarm)
     {
         Insert (Blacklist, Node-ID);
         Propagate (Blacklist);
      }
 }
```

Algorithm I. Cluster-head operation and decision making Pseudo-code

TABLE I. Wireless sensor network simulation parameters

No	Parameters	Values
1	Number of nodes	20/40/60/80/100
2	Size of network	100 * 100 m^2
3	Routing protocol	AODV
4	MAC protocol	802.11
5	Type of traffic	CBR
6	Packet size	70 byte
7	Clustering method	Static / Dynamic (LEACH)
8	Number of Cluster	2 / 3 / 4 / 5
9	Queue Length	50
10	Type of nodes	Mica2
11	Sensing Power	0.015 w
12	Processing Power	0.024 w
13	Sleep Power	0.0001 w
14	RX Power	0.024 w
15	TX Power	0.036 w
16	Initial Energy of nodes	1 j
17	Antenna Model	Omni Antenna
18	Channel Type	Wireless Channel
19	Radio Propagation Model	Two Ray Ground

TABLE II. Attacks simulation parameters

No	Parameters	Values
1	Number of attacker	1 / 2 / 3
2	Initial Energy of nodes	10 j
3	Transfer rate of packets	Between 0.01 to 0.1
4	Attacker location	Random / manual

TABLE III. Thresholds of various attacks detection

No	Threshold	Values
1	$Threshold_{RSSI}$ of All attacker	7.2E-07
2	$Threshold_{IRP}$ of DoS attack	0.15
3	$Threshold_{PDR}$ of Sinkhole attack	0.5
4	$Threshold_{PDR}$ of Selectforward	0.12
5	$Threshold_{RMI}$ of HelloFlood attack	0.15
6	$Threshold_{Alarm}$ of CH for detect	3 to 5

V. SIMULATION AND RESULTS

This section first simulates network layer and routing attacks, as presented in Section II. Then, the proposed IDS is simulated and the results are compared with the existing work.

A. Simulation of WSN and attacks

The evaluation of our IDS is performed using the network simulator NS2. The NS2 simulator is one of the most popular network simulators. The NS2 simulator is simply a discrete event simulation tool for studying the dynamic nature of communication networks and supports a wide range of protocols in all layers [34].

In this simulation, the basic network parameters are determined according to the nature of WSNs, existing requirements and the usual applications of these networks. In this scenario, our experimental

model is built on a network containing 20-100 nodes in 2-5 clusters in an area of 100 * 100 m^2 with CBR traffic and packet size of 70 bytes. The simulation parameters used in our simulation model are summarized in the Table I.

Network layer attacks cause disturbances in the routing process in WSNs. So, in order to simulate them in NS2 and apply their behavior and operation to the WSN, that's enough to simulate the functionality of the attackers by modifying the routing protocol of the attacker nodes located in the AODV.h and AODV.cc files [34], [35]. Table II presents the parameters for the simulation of attacks.

Also, in view of the points mentioned in Section IV.A to determine the thresholds of the proposed IDS, based on the simulated network with the parameters of Tables I and II, the expected thresholds are given in Table III.

B. Simulation of the proposed IDS

In order to evaluate the performances of the proposed IDS, the following criteria are considered:

Detection Rate (DR): The detection rate or the accuracy of detecting is the percentage of detected attacks relative to the total attacks.

$$Detection\ Rate\ = \frac{No.of\ Detected\ Attacks}{No.of\ Attacks} * 100\% \quad (6)$$

False Alarm Rate (FAR): This criterion shows an incorrect alarm rate in detecting attacks. In other words, it determines how much of the detected attacks was not attack, and the IDS mistakenly detected them.

$$False\ positive\ Rate = \frac{No.of\ misdetected\ Attacks}{No.of\ Normal\ connections} * 100\% \quad (7)$$

Average energy consumption*:* This criterion shows the average energy consumption in network nodes.

$$Average\ energy\ Consumption = \frac{\sum_{i=1}^{nodes} Initial\ Energy_i - Residal\ Energy_i}{No.of\ \ nodes} \quad (8)$$

End-to-end delay: This criterion is the time it takes to send a packet over the network from the source to the destination.

Network Throughput: This criterion expresses the amount of data received in the entire network in the unit of time and is calculated by the following formula.

$$Throughput = \sum_{f=1}^{Max\ Flow} \frac{received\ packets * Packet\ size * 8}{flow\ time} \quad (9)$$

***Packet Delivery Ratio (PDR)*:** This criterion specifies the amount of data received relative to the data transmitted over the entire network.

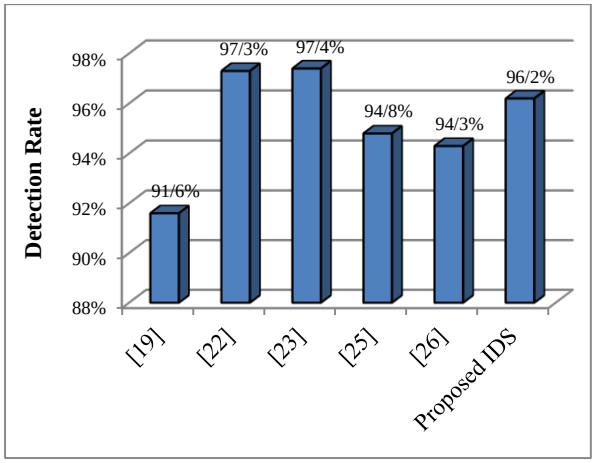

Fig. 7. Detection rate of proposed IDS and other IDSs

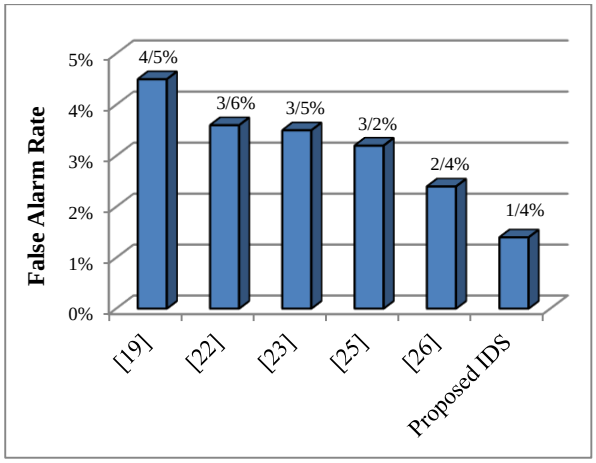

Fig. 8. False alarm rate of proposed IDS and other IDSs

$$Packet\ Delivery\ Ratio = \frac{No.of\ received\ packets}{No.of\ sent\ packets} * 100 \quad (10)$$

Routing Overhead (RO): This criterion describes the amount of overhead caused by routing data between sensor nodes in the network.

$$Normalized\ Routing\ Overhead = \frac{No.of\ Routing\ packets}{No.of\ Received\ packets} \quad (11)$$

Packet Loss Ratio: This criterion determines the percentage of packets removed relative to the send packets.

$$Packet\ Loss\ Ratio = \frac{Packet\ Loss}{No.of\ sent\ packets} * 100 \quad (12)$$

All the results presented in following are the average of 10 performed simulation operations that duration of each simulation is set to 100s. Also, for the proper comparison of the proposed method with existing works, we used the same platform to simulate all the methods whose parameters are in Tables I and II.

According to the results presented in Figs. 7 through 9, the proposed system with a detection rate (DR) of 96.2% and a low false alarm rate (FAR) of 1.4%, as well as a low average energy consumption of 0.02 Jules, is considered as an effective and lightweight method.

As shown in Fig. 7, the DR of the proposed IDS is 96.2%, with a slight difference after [22] and [23]. However, due to the low FAR of 1.4% presented in Fig. 8, and as well as the average energy consumption less than the existing works in Fig. 9, the proposed method provides more favorable conditions than the other works. The reason for the low FAR in the proposed method is that the extracted specifications of the relevant attacks have a high separability and, by applying appropriate thresholds have also been improved the detection accuracy.

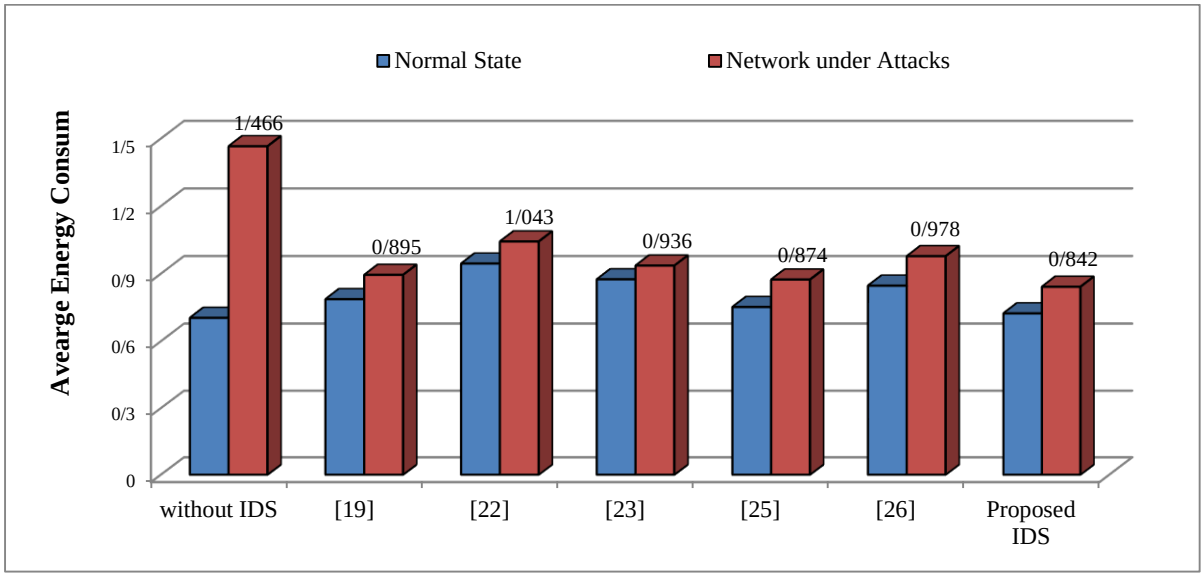

Fig. 9. Average Energy Consumption of nodes in WSN

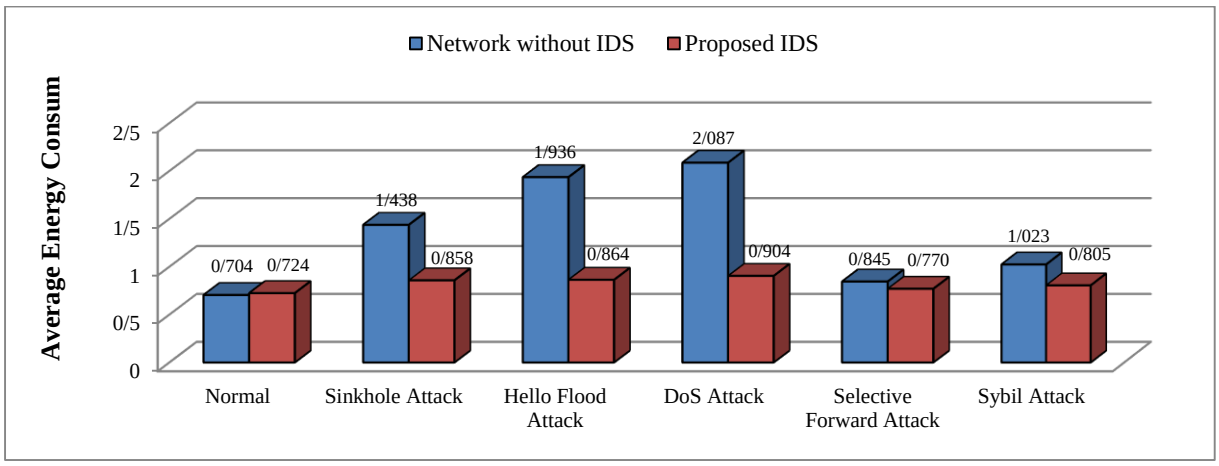

Fig. 10. Average Energy consumption of the proposed IDS against various attacks and the normal mode of the network

In order to evaluate the efficiency of the proposed IDS in terms of energy, we considered various situations:

- Network without IDS and without attacks
- Network with IDS and without attacks
- Network without IDS and under attacks
- Network with IDS and under attacks

By comparing the above scenarios in Figs. 9 and 10, it is evident that the proposed IDS is lightweight and imposes a slight overhead on the network, and also has the lowest energy consumption compared to existing methods that in WSNs It is very important. The reason for the low energy consumption of the proposed method in comparison with the existing work is that in the

TABLE IV. Comparison of proposed IDS with existing works by distinguishing between different attacks

Attack Type	**OWIDS [19]**		**GHIDS [22]**		**KBIDS [23]**		**LIDS [25]**		**ECOC [26]**		**Proposed IDS**	
	DR	FAR	DR	FAR	DR	FAR	DR	FAR	DR	FAR	DR	FAR
DoS Attack	---	---	---	---	96.2%	3.7%	96.3%	3.3%	95.2%	1.4%	95.6%	1.2%
Hello Flood Attack	92.7%	3.4%	97.2%	2.2%	98.4%	4.3%	93.9%	2.1%	96.2%	1.7%	97.5%	0.9%
Sinkhole Attack	93.4%	4.7%	96.3%	3.5%	97.6%	2.6%	94.2%	2.5%	96.1%	1.2%	94.7%	1.1%
Select Forward Attack	88.9%	5.6%	98.4%	5.1%	---	---	94.8%	4.7%	91.1%	3.4%	93.8%	2.3%
Sybil Attack	91.3%	4.3%	---	---	---	---	---	---	92.7%	4.3%	99.4%	1.7%
Total (Average)	**91.6%**	**4.5%**	**97.3%**	**3.6%**	**97.4%**	**3.5%**	**94.8%**	**3.2%**	**94.3%**	**2.4%**	**96.2%**	**1.4%**

proposed method, we have used a series of simple rules related to the extracted specifications, which leads to a significant reduction in energy consumption.

Table IV also shows the detection rate and the false alarm rate by distinguishing between different attacks in the proposed IDS compared to existing works.

In Figures 10-15, the proposed IDS is evaluated according to various performance criteria in WSNs, separately from attacks.

As shown in Fig. 11, one of the destructive effects of DOS and Hello flooding attacks is a very high delay in data transmission, which greatly reduces the network performance, but by employing the proposed IDS and timely detection of these attacks, Delay has returned to its normal state.

The effect of various attacks on the throughput and packet delivery ratio is also seen in Figures 12 and 13, a hello flooding attack with a large increase in routing overhead causes high delay to sending data in nodes, which results in a significant decrease in throughput and PDR. In a sinkhole attack, too, since the traffic sent by the nodes to the attacker's node is eliminated without passing through it, the throughput and PDR in the network is greatly reduced. Finally, as you can see, using the proposed IDS returns the throughput and PDR to the normal level.

As shown in Fig. 15, another destructive effect of the hello flooding attack compared to other attacks is the sending of many communication messages to other nodes, which causes a significant increase in network RO, but by the proposed IDS, the RO goes back to the normal state.

With regard to the shapes and the comparison of the network status in the presence and absence of the proposed IDS, it is observed that different attacks are greatly reduced network performance. Also By applying the proposed IDS, the efficiency and performance of network maintained in the appropriate level.

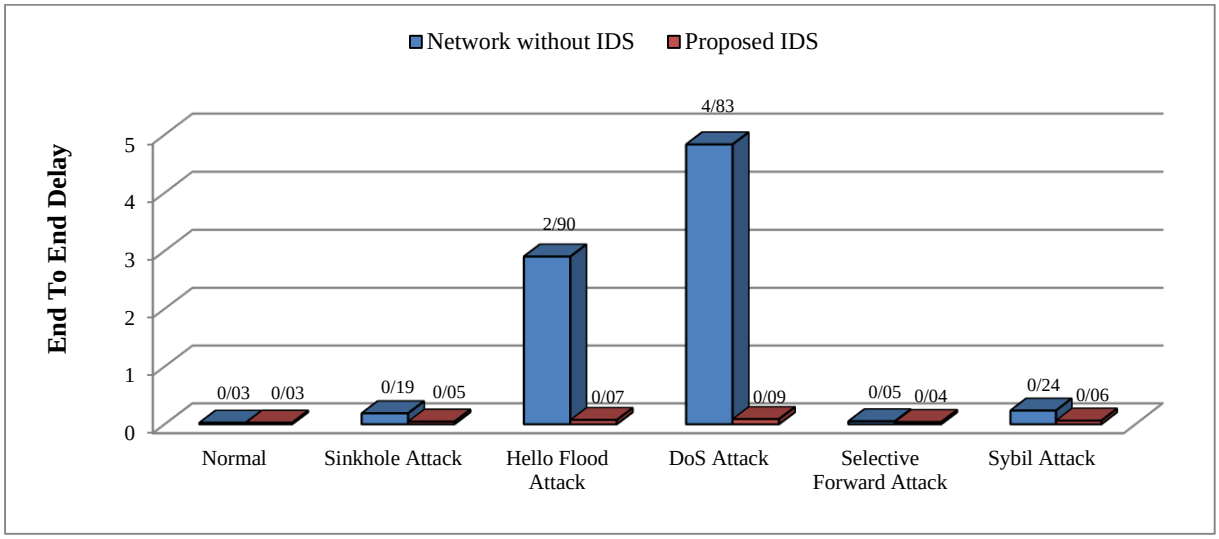

Fig. 11. End to end delay of the proposed IDS against various attacks and the normal mode of the network

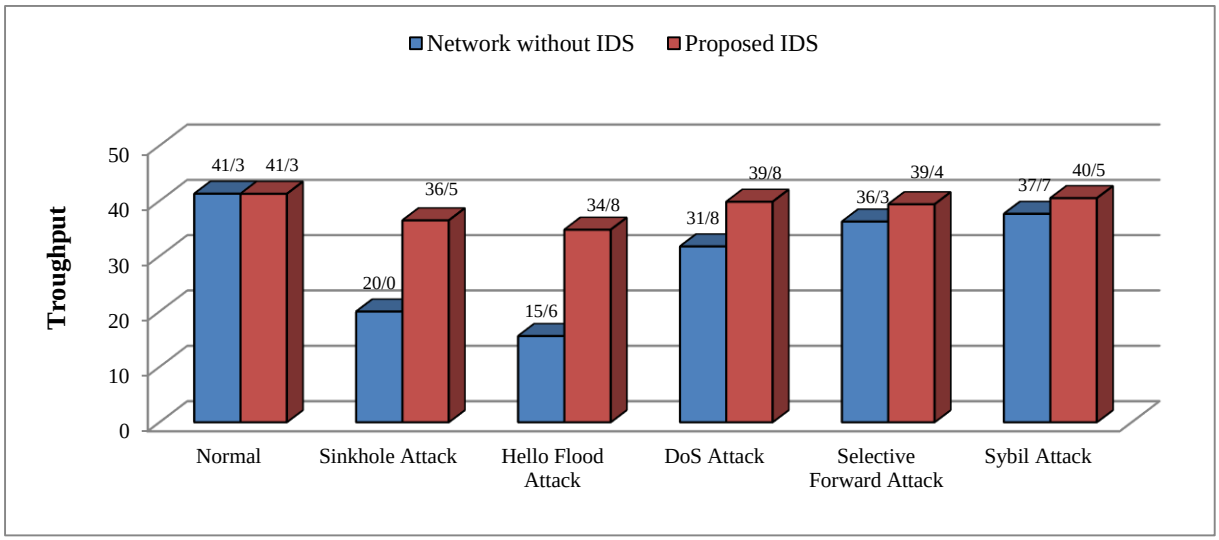

Fig. 12. Throughput of the proposed IDS against various attacks and the normal mode of the network

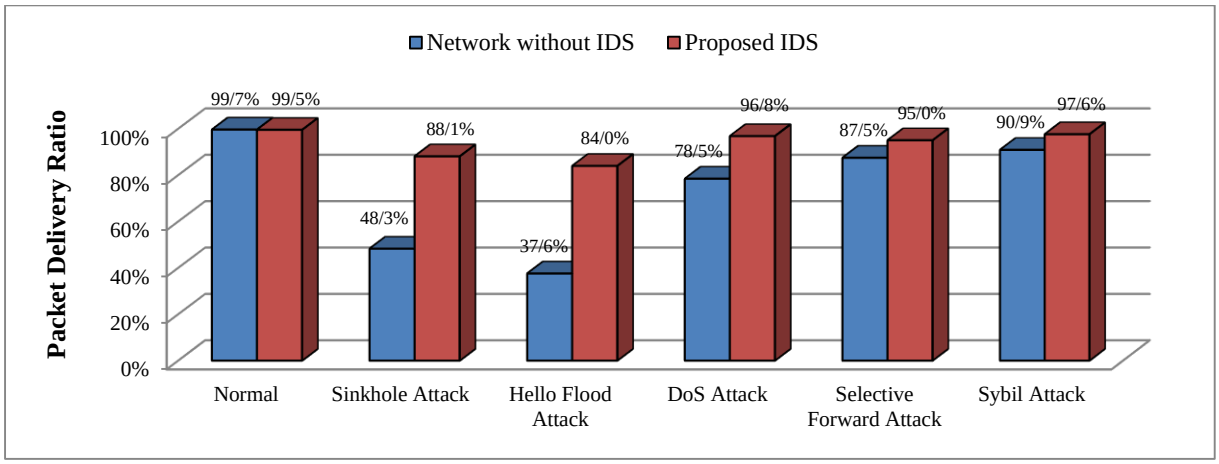

Fig. 13. Packet delivery ratio of the proposed IDS against various attacks and the normal mode of the network

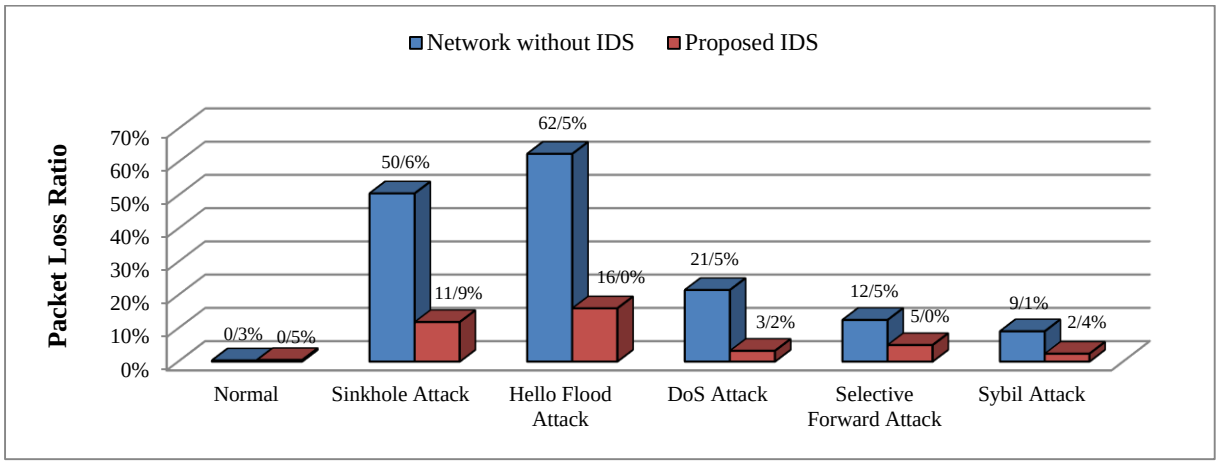

Fig. 14. Packet loss ratio of the proposed IDS against various attacks and the normal mode of the network

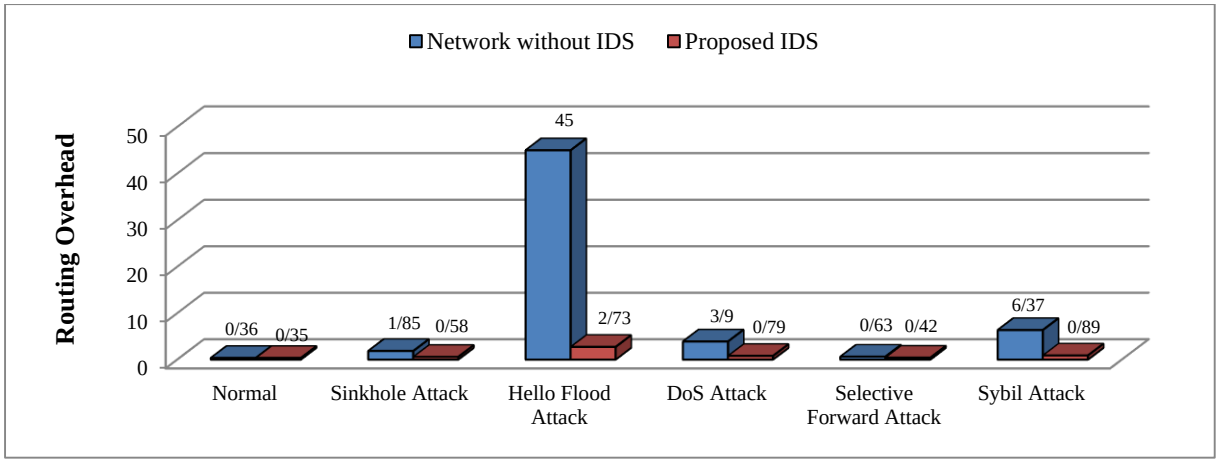

Fig. 15. Routing overhead of the proposed IDS against various attacks and the normal mode of the network

VI. CONCLUSION

In this paper, we first introduced the common attacks on WSNs and then examined the existing IDSs to deal with them. We then introduced a lightweight IDS to detect network layer and routing attacks, in which we considered the characteristics of various attacks (based on the analysis of the behavior of the attacks in Section II.A) for detection. The proposed system covers all network layer and routing attacks in WSNs compared to existing works that often focus on a specific attack. Finally, we evaluated the proposed system with all performance criteria. The results obtained from simulations show that the proposed IDS with a detection rate of 96.2% and a low false alarm rate of 1.4%, as well as a low average energy consumption of 0.02 Jules, as an effective and lightweight method for the WSNs, is well-known, and with its application in WSNs, the performance of the network can be kept in the optimum level.

REFERENCES

[1] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] J. Sen, "A Survey on Wireless Sensor Network Security", *International Journal of Communication Networks and Information Security. (IJCNIS)*, vol. 1, no. 2, pp. 55-78, Aug. 2009.

[3] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6-28, Third Quarter 2008.

[4] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52-73, Second Quarter 2009.

[5] G. Padmavathi and D. Shanm, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *International Journal of Computer Science and Information Security*, vol. 4, no. 1, pp. 1-9, Aug. 2009.

[6] Y. Maleh and A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network", *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 5, no. 6, Dec. 2013.

[7] E. J. kumar Patel and K. Tripathi, "Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODV Protocol", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 5, pp. 9660-9669, May 2016.

[8] V. C. Manju, "Sybil Attack Prevention in Wireless Sensor Network," *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)*, vol. 4, no. 2, pp. 125-132, Apr. 2014.

[9] M. A. Salam and N. Halemani, "Performance Evaluation of Wireless Sensor Networks Under Hello_Flood Attack," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 8, no. 2, pp. 77-78, Mar. 2016.

[10] A. Liu, M. Dong, K. Ota, and J. Long, "PHACK- An Efficient Scheme for Selective Forwarding Attack Detection in WSNs," *Sensors*, vol. 15, no. 12, pp. 30942-30963, Dec. 2015.

[11] S. Patil and S. Chaudhari, "DoS Attack Prevention Technique in Wireless Sensor Networks," *Procedia Computer Science*, vol. 79, pp. 715-721, Dec. 2016.

[12] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266-282, First Quarter 2014.

[13] A. Ghosal and S. Halder, "A survey on energy efficient intrusion detection in wireless sensor networks," *Journal of Ambient Intelligence and Smart Environments*, vol. 9, no. 2, pp. 239-261, Feb. 2017.

[14] S. Duhan and P. Khandnor, "Intrusion detection system in wireless sensor networks: A comprehensive review," *2016 International Conf. on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, pp. 2707-2713, 2016

[15] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," *International Journal of Distributed Sensor Networks*, vol. 2013, no. 4, pp. 1-7, May 2013.

[16] S. Shin, T. Kwon, G. Jo, Y. Park, and H. Rhy, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744-757, Nov. 2010.

[17] C.C. Su, K. M. Chang, Y. H. Kuo, and M. F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks]," *IEEE Wireless Communications and Networking Conference, 2005*, New Orleans, LA, vol. 4, pp. 1927-1932, 2005

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

[19] C. F. Hsieh, R. C. Chen, and Y. F. Huang, "Applying an Ontology to a Patrol Intrusion Detection System for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2014, no.2, pp. 1-14, Jan. 2014.

[20] F. Hidoussi, K. Lakhtaria, H. Toral-Cruz, A. Mihovska, and M. Voznak, "Centralized IDS Based on Misuse Detection for Cluster Based Wireless Sensors Networks," *Wireless Personal Communications Journal*, vol. 85, no. 1, pp. 207-224, May 2015.

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

[22] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks." *Procedia Computer Science*, vol. 52, pp. 1047-1052, June 2015.

[23] H. Qu, Z. Qiu, X. Tang, M. Xiang, and P. Wang, "An Adaptive Intrusion Detection Method for Wireless Sensor Networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 11, pp. 27-36, 2017.

[24] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," *International Symposium on Networks, Computers and Communications*, Marrakech, , pp. 1-6, 2017

[25] H. Zhou, Q. Liu, and C. Cui, "Research on Intrusion Detection Algorithm Based on Multi-Class SVM in Wireless Sensor Networks," *Communications and Network*, vol. 5, no. 3, pp. 524-528, Sep. 2013.

[26] Y. Maleh and A. Ezzati, "Lightweight Intrusion Detection Scheme for Wireless Sensor Networks," *IAENG International Journal of Computer Science*, vol. 42, no. 4, pp. 347-354, Dec. 2015.

[27] M. Mirzasadeghi and H. Bakhshi, "A New Method for Clustering Wireless Sensor Networks to Improve the Energy consumption," *Journal of Communication Engineering*, vol. 5, no. 2, pp. 136-149, Dec. 2016.

[28] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14, pp. 2826-2841, Oct. 2007.

[29] S. K. Gupta, N. Jain, and P. Sinha, "Clustering Protocols in Wireless Sensor Networks: A Survey," *International Journal of Applied Information Systems (IJAIS)*, vol. 5, no. 2, pp. 41-50, Jan. 2013.

[30] S. S. Wang, K. Q. Yan, S. C. Wang, and C. W. Liu, "An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks," *Expert Systems with Applications*, vol. 38, no. 12, pp. 15234-15243, Dec. 2011.

[31] M. Bajelan and H. Bakhshi, "An Adaptive LEACH-based Clustering Algorithm for Wireless Sensor Networks," *Journal of Communication Engineering*, vol. 2, no. 4, pp. 351-365, Autumn 2013.

[32] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Application specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Networking*, vol. 1, no. 4, pp. 660-670, Oct. 2002.

[33] M. Demirbas and Youngwhan Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," *International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*, Buffalo-Niagara Falls, NY, pp. 570-574, 2006.

[34] K. K. Waraich and B. Singh, "Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks," *International Journal of Advanced Science and Technology*, vol. 82, pp. 63-70, Sep. 2015.

[35] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs," *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, pp. 1181-1187, 2012.