Indian Journal of Science and Technology, *Vol 12(3), DOI: 10.17485/ijst/2019/v12i3/140767, January 2019*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

XLID: Cross-Layer Intrusion Detection System for Wireless Sensor Networks

Manal Alharthi and Manal Abdullah

Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, KAUJeddah, Saudi Arabia; m.manal-@hotmail.com, maaabdullah@kau.edu.sa

Abstract

Objectives: This research developed an IDS based on cross layer interaction between network, and MAC layers of OSI model. XLID is checked against other traditional (non-cross-layered) IDS that are based on single layer protocol. **Methods/ Statistical Analysis**: For this purpose, a simulator was built specifically for simulating the proposed approach. XLID showed its superiority in terms of number of detected intruders, power consumption, and throughput, over other non-cross-layered IDS. **Findings:** Based on the results XLID enhanced the intrusion detection rate by 42% on average, 75% higher throughput to base station, and a 23% reduction of power consumption compared to non-cross-layered IDS. Moreover, the total energy saved during simulation time ranges from 25% up to 45% compared to non-cross-layered IDS. **Application/Improvements:** Findings pointed out that, the detection rate at Network layer ranges from 5% up to 18% compared to non-cross-layered IDS, while it is from 2% up to 15% in the MAC layer.

Keywords: Cross-Layer Intrusion Detection, Intrusion Detection System (IDS), Security Attacks, Wireless Sensor Networks (WSNs)

1. Introduction

Wireless Sensor Network (WSN) is a sort of system that have many (from handfuls to thousands) minor gadgets, detecting and gathering point by point data about a physical situation. These modest sensors are primarily little estimated and have low power, low preparing capacity and minimal effort. WSNs arrange must be adaptable, solid, secure, self-association and have adaptation to non-critical failure[1]. These networks are composed of sensor nodes and sinks. The main objective of a sensor node is to collect information from its surrounding environment and transmit it to the sink. WSNs are conveyed in physical cruel and threatening conditions where hubs are constantly presented to physical security dangers harms. Moreover, self-sorting out nature, low battery control supply, restricted transmission capacity bolster, circulated tasks utilizing open wire-less medium, multi-bounce traffic sending, and reliance on different hubs are such qualities of sensor organizes that open it to numerous security assaults at all layers of the OSI demonstrate[2]. Numerous security-related answers for WSNs have been proposed, for example, validation, key trade, and secure steering or security systems for explicit assaults. These security systems are equipped for guaranteeing security at some dimension; in any case, they can't dispose of the majority of the security assaults. An Intrusion Detection System (IDS) is one conceivable answer for location a wide scope of security assaults in WSNs[2].

An IDS is additionally alluded to as a second line of resistance, which is utilized for interruption identification just; that is, IDS can identify assaults yet can't counteract or react. When the assault is recognized, the IDSs raise a caution to advise the controller to act. There are two imperative classes of IDSs. One is rule-based IDS and the other is irregularity-based IDS. Standard based IDS are otherwise called mark-based IDS which are utilized to distinguish interruptions with the assistance of implicit marks. Principle based IDS can recognize surely understood assaults with incredible precision, yet it can't

*Author for correspondence

identify new assaults for which the marks are absent in interruption database. Peculiarity based IDSs identify interruption by coordinating traffic examples or asset usages. Albeit peculiarity based IDSs can recognize both understood and new assaults, they have false positive and false negative alerts. Some IDSs work in explicit situations or with specific steering conventions. Watchers work with proactive steering convention to distinguish directing peculiarities. It is executed on every hub, so every one of the hubs require a type of participation to recognize directing interruptions[3-5]. A large portion of the security conventions depend on specific presumptions about the idea of assaults.

The layered methodologies have detectable weaknesses, for example, the excess as well as firmness of the security arrangements, which made the layers security arrangements frequently wasteful and insufficient. It was, be that as it may, valuable to build the security approach for the WSNs dependent on cross-layer collaboration between all segments in various layers of the convention stack. Therefore, these new methodologies most likely provided another guidance towards the issue of security for remote sensor systems[6].

This research mainly contributes towards the design of a cross-layer intrusion detection system (XLID). The basic idea of XLID is to detect intruders when they attempt to communicate with the network nodes. In addition, by utilizing the steering data at the MAC layer, every sensor hub can already know the wellspring of parcels that will be gotten. Accordingly, any hub attempting to speak with the sensor hubs is promptly perceived as a gatecrasher in the event that it is excluded in the steering way. For remote medium, got flag quality is identified with the separation between hubs. At the physical layer, every hub knows the flag quality of the parcel sent by its neighbors (determined beforehand by base station). In this way, the validness of the interloper hub can be distinguished as the flag quality of the bundles won't be identical to determined one. At that point, by consolidating the determined flag quality incentive with neighborhood steering table, the location capacity is altogether made strides. This study is organized as follows: In Section 2, we show some basic information necessary as a background for WSNs. After that, we went over some related work. The research assumptions and default parameters are presented in Section 3. In Section 4, we presented the proposed XLID model, then in Section 5, we presented its simulation and evaluation criteria. Finally, we discuss the results; conclude the research, and stat future work in section 6.

2. Background

WSNs confront genuine security issues, in view of the transparency of nodal sending and remote correspondence. In some WSN arrangements, the SNs might be caught and the key data may be spilled or traded off. The reason for an aggressor is to upset the security traits of WSNs, including privacy, trustworthiness, accessibility and validation. To accomplish these goals, the assailant may dispatch assaults from various convention layers of WSNs.

At the physical layer, the aggressor can stick the physical channel by meddling with the radio frequencies that hubs use for correspondence[1]. The aggressor can likewise extricate the mystery data from the caught hub, mess with its hardware, adjust the program codes, or even supplant it with a vindictive hub[2]. Assaults at the medium access control (MAC) layer mean to disturb the accessibility of the system by deliberately making impacts, acquire out of line need in the conflict for the channel or scatter the constrained vitality of hubs. However, security threats are defined as any actions that leads to violate any security issue[7]. In WSN, and due to the existence of many routing protocols, it becomes an easy target for intruders or any other sources of attacks[7]. Three main type of WSN intrusion detection techniques were discussed in[7], they are Anomaly detection, Misuse detection and Specification-based detection.

2.1 WSN Protocol Stack (Layers)

The protocol stack used by the sink and all sensor nodes is a reduced OSI model which combines power and routing awareness. It comprises of; physical layer, medium access control layer, steering layer and application layer (See Figure 1). The physical layer tends to the necessities of straightforward yet powerful tweak, transmission, and getting methods. The MAC layer is in charge of guaranteeing dependable correspondence through blunder control procedures and oversee channel access to limit impact with neighbors communicates. The directing layer deals with steering the information and relying upon the detecting assignments, diverse kinds of utilization programming can be fabricated and utilized on the application layer.

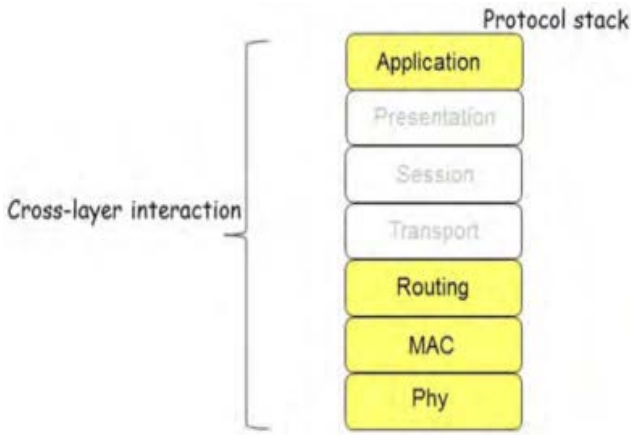

Figure 1. OSI model of WSN (Protocol Stack).

2.2 Intrusion Detection System (IDS)

An IDS is likewise alluded to as a second line of barrier, which is utilized for interruption recognition just; that is, IDS can distinguish assaults yet can't avert or react. When the assault is recognized, the IDSs raise an alert to educate the controller to act.

IDS have three principle parts, they are[2]:

- Monitoring part is utilized for nearby occasions checking and additionally neighbors observing. This part generally screens traffic designs, inward occasions, and asset usage.
- Analysis and recognition modules are the primary part which depends on displaying calculation. System tasks, conduct, and exercises are investigated, and choices are made to pronounce them as pernicious or not.
- Alarm part is a reaction producing segment, which creates a caution in the event of location of an interruption.

There are two imperative and surely understood classes of IDSs (2): One is known as signature-based IDS, where the marks of various security assaults are kept up in a database. The second sort is oddity-based IDS. This sort is successful to recognize new assaults; nonetheless, it now and again misses to distinguish surely understood security assaults.

The reason is that oddity based IDSs don't keep up any database, however they persistently screen traffic examples or framework exercises. Wireless sensor systems are helpless against assortment of assaults at various convention layers. In the current interruption location plans, cross-layer assaults are only here and there considered.

In order to identify malicious nodes more efficiently, a few examinations have been proposed in this space where most offer interruption identification instruments committed to impromptu systems. Subsequently, they consider the imperatives and constraints of WSNs. There is some exploration endeavoring to adjust the arrangements recently proposed to WSNs and propose new arrangements devoted for them. IDS systems proposed by[9] and[6] contain certain screen hubs in the system which are mindful of checking their neighbors, searching for gatecrashers. They tune in to messages in their radio range and utilize a cushion to store explicit message handle that may be valuable to an IDS framework running inside a sensor hub, yet no subtleties are given concerning how this framework functions. In these models, there is no joint effort among the screen hubs. The two papers lead to reason that the cushion measure is an imperative factor that incredibly influences the rate of false alerts.

Two more IDSs for directing assaults in sensor systems are portrayed by[10] and[11]. They expect in the two papers that directing conventions for impromptu systems can likewise be connected to WSNs: [10]accept the AODV (Ad hoc On-Demand Distance Vector) convention while[12] utilize the DSDV and DSR conventions. Interlopers' identification utilizes explicit qualities of these conventions like "number of course asks forgot". However, as far as anyone is concerned, these steering conventions are not alluring for sensor systems. Consistent observing may expend vitality, which isn't alluring in WSNs. subsequently; a group based identification approach for WSNs is proposed in[13]. In this methodology, a system is isolated into groups. Each group head screens its bunch individuals. Every one of the individuals in a bunch is additionally separated into gatherings and the gatherings alternate to screen the group head. The general system vitality cost is diminished in light of the fact that not all the sensor hubs continue observing.

Sinkhole assaults can be recognized through the calculation proposed by creator in[14], even in nearness of conspiring hubs. The initial step comprises of finding a rundown of suspected hubs through assessing the assaulted region. Creators accept that the base station has an unpleasant comprehension on the area of hubs, e.g. acquired through different limitation systems. Also, the interloper will be distinguished through breaking down the steering design in the influenced region. In detail, a

demand message containing the IDs of every single influenced hub is communicated by base station. A timestamp is incorporated into a demand marked with the private key of the base station to avert replay assaults. The influenced hub answers with its very own ID, the ID of the following jump hub and the steering cost (e.g. jump check) to that hub on getting the demand. The answer message is sent along the invert way in the communicate, as the following bounce and steering cost could as of now be influenced by the assault. At the base station, building a tree utilizing the following jump data permits to examine the directing example. In a sinkhole assault, all system traffic stream towards a similar goal which uncovers the character of the interloper. In[6] Each hub outfitted with IDS should work autonomously and distinguish interruptions locally.

No coordinated effort exists with different hubs. The hubs own directing table and all bundles the hub got are the main data utilized. A lot of twelve highlights to recognize steering abnormalities in an assortment of directing conventions are distinguished by the creators.

Two validation systems are utilized to avoid interruptions, one for control messages, (for example, directing messages) and the other for detected information in[15]. To identify interruption, assault the creators execute a cooperation-based IDS to screen bunch heads and in addition part hubs. An IDS to recognize the blackhole and the particular sending assault is proposed in[16]. So as to distinguish the aggressor, each hub screens its neighborhood and works together with its closest neighbors. They can recognize deviations from typical conduct by following a standard based methodology (rate of messages dropped over a specific limit); the aggressor hub is distinguished, if the greater part of the guard dog hubs raises a caution for this hub. This methodology is stretched out in[17], so as to identify sinkhole assaults. In the methodology of[18], the conduct of the quick neighbors is checked by every sensor. The calculation considers numerous qualities at the same time in hub conduct assessment, without requiring earlier information of what typical/irregular conduct is. In[19], creators proposed a structure of a machine learning based interruption identification framework. An interruption recognition specialist is executed by every hub to catch the traffic of its neighbors, yet there is no participation among hubs to identify aggressors. The ID specialist starts the discovery procedure by distinguishing if the hub itself is assaulted. For this reason, a nearby Intrusion Detection Component (LIDC) was proposed to break down nearby highlights (bundle impact proportion, parcel conveyance holding up time, RTS parcels rate, neighbor tally, steering cost, control utilization rate, detecting perusing report rate...). In[20] that is ad-hoc networks of wireless devices deployed on (or in proximity of, creators present a half breed IDS, which speaks to a blend of brought together and decentralized IDS. In this design, ID is performed both locally and universally. The detail of how inconsistencies can be recognized isn't depicted by the creators. Creators In[21] proposed an IDS dependent on bunched sensor organizes and can distinguish a few directing assaults, in light of neighbor learning and steering rules. In their design, an IDS operator is contained in each hub which has a place with a solitary group. There are two interruption modules, a nearby and worldwide IDS operator. Sent and got bundles by the hub are checked by nearby operator. Furthermore, a rundown about noxious hubs in the system (boycott) is kept. Correspondence of the neighboring hubs is observed by the worldwide specialist. The caught correspondence is checked utilizing pre-characterized and two-bounce neighbor information, and this to identify inconsistencies.

3. Research Assumptions

In this research, the fundamental thought is the utilization of cross layer connection idea to distinguish diverse kinds of assaults on a few layers of the OSI demonstrate. This is to create XLID: Cross-Layer Intrusion Detection show. In this proposed framework, the MAC layer utilizes the cross-layer data from system and physical layers so as to identify conceivable interruptions. Furthermore, the system layer utilizes the neighboring directing data to distinguish the wellspring of the parcel and stamped it as vindictive development.

When interruption is distinguished, different sorts of activities (like dropping a bundle, hailing a neighbor and so on.) can be taken. Be that as it may, in this exploration, we center just on interruption identification and consequently don't examine answers for handle interruptions. Also, building up an IDS works on various layers of the OSI show. So as opposed to offering IDS for each layer, XLID has built up a solitary interruption location framework that can recognize diverse kinds of assaults on a few layers of the OSI demonstrate utilizing cross-layer ideas (mostly focusing on Network and MAC layers).

3.1 WSN Communication Model

It is important before going through XLID to explain briefly main model architecture and components of WSN. WSN consists mainly of a base station BS, some clusters including sensor nodes as cluster members, and each cluster has one node as cluster head CH, as can be shown in Figure 2. BS can communicate with computers at other locations which may be an "End-user" terminal connected through the Internet. WSNs are useful when data needs to be gathered from large and/or remote areas. Information such as temperature, pressure and sound can be measured and monitored, especially in unforgiving environments and hostile conditions.

Each remotely deployed sensor node in WSN model is powered by a small battery. Depending on power requirements of the desired application, a battery can last for days, months or even years[22]. However, this energy source is expectedly limited. When the battery is depleted, a sensor node will be rendered useless. With a setup as in Figure 2, one of the important sensors is the cluster head (CH). An unavoidable process in such a setup is the re-election of a new CH when the existing one's energy falls below a certain threshold. This re-election task consumes energy that decreases the WSN's overall lifespan[23].

3.2 Security and Attacks Assumptions

In this research, it is assumed that correspondence between the system hubs and the base station is anchored utilizing security conventions dependent on symmetric keys. Security in WSN display comprises on setting up keys following a pre-circulated approach which appears to be increasingly fitting for sensor systems[22]. In this methodology (mystery) key data is disseminated to all sensor hubs before arrangement. In XLID model, two types of traditional IDS are applied along with the proposed IDS, they are: Inconsistency based IDS, and Signature based IDS. The characterization depends on heuristics or standards, as opposed to examples or marks, and endeavors to distinguish any kind of abuse that drops out of ordinary framework activity[24-25]. In this research, we apply this type of intrusion to detect anomalies that affects the behavior of the network, usually the attack takes place in the MAC layer.

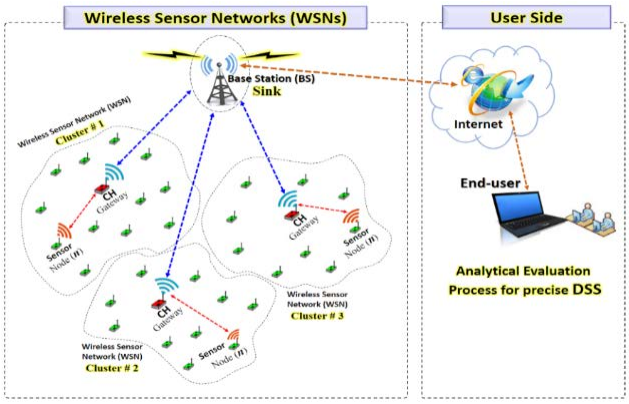

Figure 2. Wireless Sensor Network architecture.

4. Methodology

4.1 Proposed XLID Model

Cross Layer Intrusion Detection XLID model depends on a cross layer design that misuses cooperation and coordinated effort of two neighboring layers in the OSI display i.e. System, and Mac layers. The fundamental thought of XLID is to recognize interlopers when they endeavor to speak with the system hubs. In the wake of getting RTS parcels of the gatecrasher hubs by the focused on hub, XLID identification framework checks on the off chance that it is one of the neighbors in the steering way (by counseling the directing table at the system layer). In addition, by using the routing information at the MAC layer, every sensor hub can already know the wellspring of parcels that will be gotten. Accordingly, any hub endeavoring to impart (get RTS or CTS bundle) with the sensor hubs is quickly perceived as a gatecrasher on the off chance that it is excluded in the steering way. For remote medium, got flag quality is identified with the separation between hubs. At the physical layer, every hub knows the flag quality of the bundle sent by its neighbors (determined already by the base station).

Along these lines, the legitimacy of the gatecrasher hub can be distinguished as the flag quality of the parcels won't be equal to determined one. At that point, by consolidating the determined flag quality incentive with neighborhood steering table, the recognition capacity is essentially made strides. A pseudo code of XLID intrusion system is stated in Algorithm 1. For simplicity a pictorial view in a flow chart represents the pseudo code of Algorithm 1 is shown in Figure 3.

4.2 XLID Signaling Information

Information exchange between numbers of layers of the stack protocol is required for different optimization solu-

Algorithm : Cross-Layer Intrusion Detection
Input: A request to Send a Frame

```
Step 1. Begin
Step 2. Network Setup and Start Sensing
Step 3. While (there is still a living nodes in the WSN) Do          // Mac Layer Intruder
        { Receive a request to send a frame;
          Establish a connection by CTS and RTS packets;
          If (the Identity of the received request is unknown) then
            { Deny the request;
              Intruder Counter is Incremented;
              Intruder Alert is Raised;
              Jump to Step 4
            }   // end if
        Else
          If (the requested node tries to integrate itself to the routing table) then   // Network Layer Intruder
            { Check its existence in the neighboring routing table;
              If (node is not exists) then
                { Deny the request;
                  Intruder Counter is Incremented;
                  Intruder Alert is Raised;
                  Jump to Step 4
                }   // end if
              Else
                { Normal Situation }
            }   // end if
          Else
            { Normal Node }
        }  // End of While
Step 4. Stop Simulation
Step 5. Generate Reports
```

Algorithm 1. XLIDS Model Algorithm

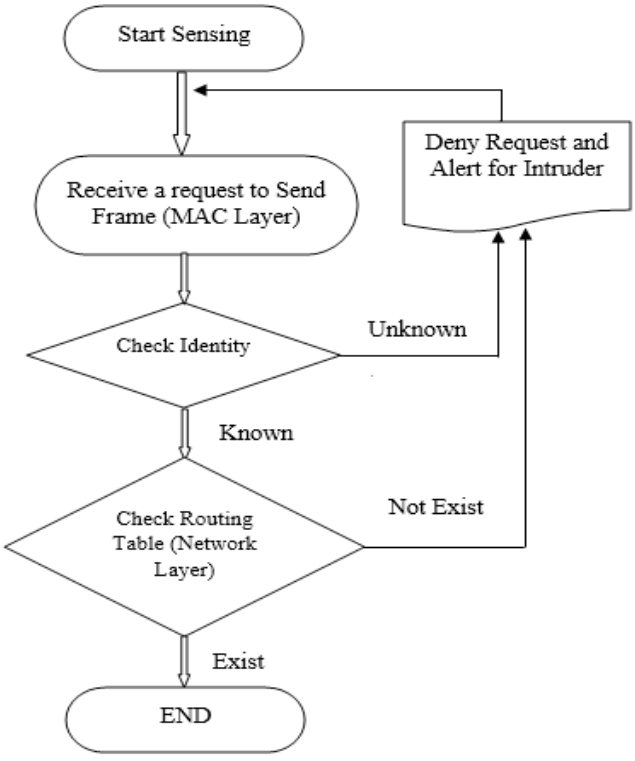

Figure 3. XLID Proposed Cross-Layer Intrusion Detection Flow Chart.

tions. Cross layer design solution implementation inside reference model of TCP/IP protocol is a common cross-layer signaling model used for their interoperability and coexistence. The architecture of XLID maintains the traditional layered architecture and adopts the principle of communication via a cross layer module. The nearness of cross-layer module gives a cross layer singular advancement and proceeds to the two layers and the module itself without irritating the general framework. Another favorable position is that this module has a free access to every one of the layers, settling on choices increasingly objective. It likewise permits simple and straightforward joining of new cross layer calculations and information without changing whatever is left of the engineering. Figure 4 demonstrates the cross-layer proposed engineering. The intrusion detection architecture includes essentially two parts: the interaction interface and cross-layer data module.

4.3 Information Interchange between Layers in XLID

XLID works at MAC layer level by misusing directing data. Therefore, adjustments are made in RTS and

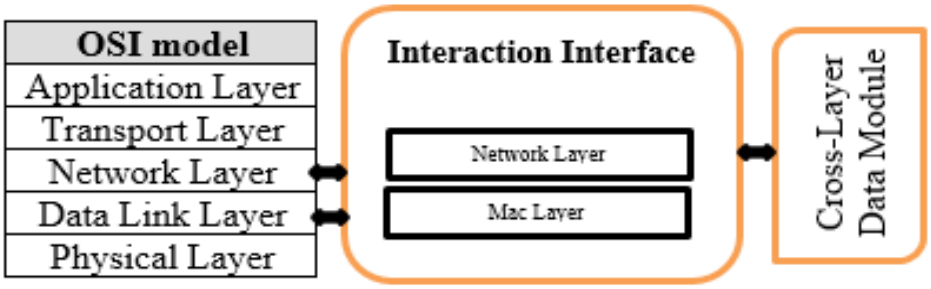

Figure 4. Proposed XLID Architecture.

CTS message structures without abuse the IEEE 802.11 standard. The Sink hub deliver should be known at the dimension of every hub of the system.

Exchanging data between TCP/IP Protocol Suit layers is achieved using direct inter-layer -Internet control message protocol (ICMP). ICMP is the pattern of direct inter-layer communication performed at any of the protocol stack, it is not explicit. Consequently, in the interaction interface part, the MAC provide a service to the upper layer (Network Layer) and provide it with the Request to Send (RTS) packet after validating its identity.

4.4 Generating Targeted Attacks

In order to test the suggested model, a reasonable data set called NSL-KDD(25) which is a new version of Dcup99 dataset(25). The only data required is just the attacks types and names considered in the data set. Attacks at the system layer expect to disturb the system directing and obtain or control the information streams. Models are mock directing data, specific parcel sending, sinkhole, wormhole, blackhole, sybil, and hi surge assault. Assaults at MAC layer plan to upset the accessibility of the system by deliberately making impacts, acquire out of line need in the conflict for the channel or scatter the constrained vitality of hubs. Assaults at the MAC layer incorporate crash, forswearing of rest, Guaranteed Time Slot (GTS) assault, back-off control, etc.

5. XLID Simulation and Performance Evaluation

In this section, a performance analysis is conducted in order to explore the performance of the proposed XLID. Simulation experiments will extract multiple percentage including number of detected attacks, and the energy consumed by both cross-layered and non-cross-layered methods. The objectives and goals of experimental analysis are to investigate the results of the proposed approach. A full simulator was implemented using MATLAB to simulate the XLID model and to collect performance data then analyze it. The next subsections show the simulator interface, and a set of experiments performed by this simulator. Analysis and comparisons have been carried out based on the collected data by the simulator. The analysis goal is to verify the suitability and superiority of XLID over traditional IDS.

5.1 Simulation Environment

To evaluate XLID, a reproduction situation with a component of 150 x150 m2 is accepted to convey the detecting hubs (n=100). The hubs are arbitrarily (consistently) dispersed over the field. The sink (i.e. BS) is situated at the position (50, 75) of the field. Two intruder nodes are in the field, one is specialized in attacking MAC layer and located at position (10,140), and the other one for attacking the network layer and located at position (90,145) as illustrated in Figure 5 which is part of MATLAB simulator. The traffic type, Routing Protocol, Antenna Type, MAC layer protocol, and Channel band width are: CBR, HEEP, Omni-Antenna, SMAC, 20 Kbps respectively. The simulation parameters and the radio characteristics used in this simulation are summarized in Table 1. All system hubs begin the reproduction by an underlying vitality equivalent to 2 J and a boundless measure of information to be transmitted to the base station. Moreover, the vitality of the base station is considered as boundless. Every hub utilizes its restricted stores of vitality all through the length of recreation, which includes its exhaustion. In this manner, any hub which has depleted its vitality save is viewed as dead. In recreation demonstrate, we expected that there are 2 interloper hubs sent in the field. Every one of gatecrashers' hubs go through a time of aloof tuning in

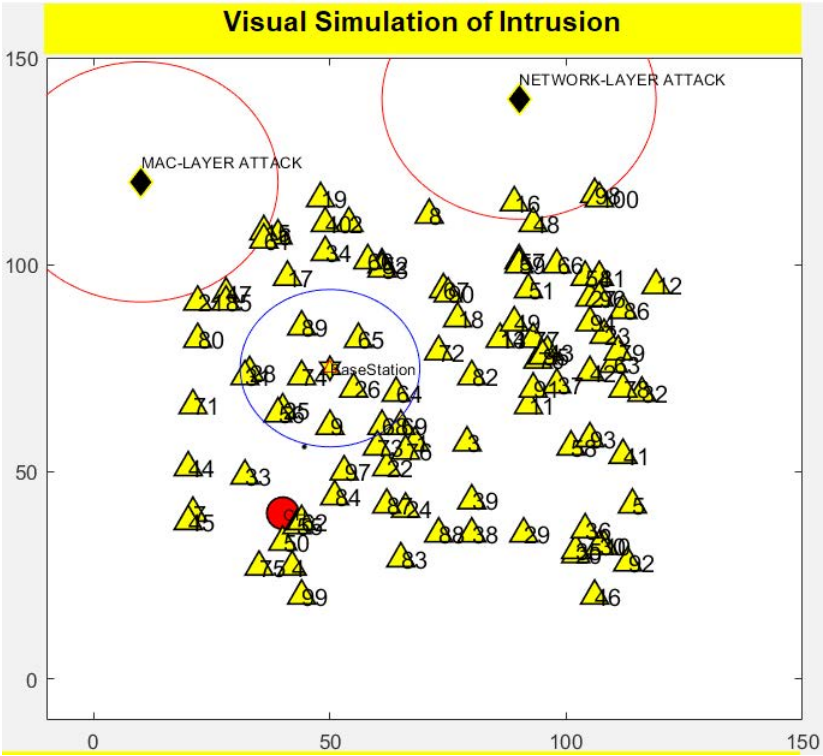

Figure 5. WSNs Topology.

Table 1. Simulation Parameters

Parameter	Meaning	Value
N	Number of nodes	100 nodes
I	Number of intruder nodes	2
P_{opt}	Optimal Election Probability of Cluster Heads	0.1
M	Percentage of Elected Cluster Heads	5%
X and Y	Field Dimension	150 X 150 m^2
Sink.X and Sink.Y	Base Station Location in the Field	50 X 75
E_0	Initial Energy	2J
E_{fs}	The Amplification Coefficient of Free-Space Signal	10 $_p$J/bit/m^2
E_{mp}	Multi-Path Fading Signal Amplification Coefficient	0.0013 $_p$J/bit/m^2
E_DA	Data Aggregation Energy	5 nJ/bit/message
E_{elec}	The energy dissipated per bit	50nJ/bit
Rmax	Maximum Number of Rounds	10000 round
MS	Message Size	4000 bit
RTS, CTS, ACK	Request to Send, Clear to Send, and Acknowledgement (Packet Size)	30 Byte

and after that attempt to associate with hubs arbitrarily focused on. All recreation results displayed later are the normal of 10 performed reenactment tasks. The span of every reenactment is set to 1000 sec most extreme.

According to the radio energy dissipation model illustrated in Figure 6 the total energy consumed by transmitting an L-bit message over a distance d, can be calculated based on equation (1).

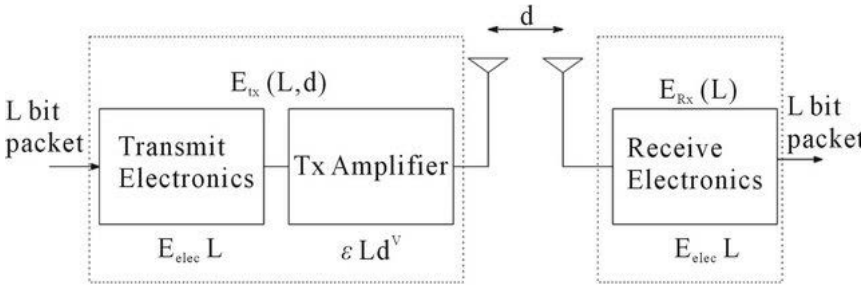

Figure 6. Radio Energy Dissipation Model.

$$E_{tx}(m,d)=\begin{cases} l*E_{elec}+l*\varepsilon_{fs}*d^2 & if\ \ d\le d_0 \\ l*E_{elec}+l*\varepsilon_{mp}*d^4 & if\ \ d\ge d_0 \end{cases} \quad (1)$$

Where, is the energy dissipated per bit, the amplification coefficient of free-space signal and is the multi-path fading signal amplification coefficient (and are the transmission ability), d is the distance from the sender to BS, and is the coverage area that is calculated as in equation (2)

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}}, at\ \ d=d_0 \quad (2)$$

To receive the L-bit message, the system expends energy as in equation (3)

$$E_S=l*E_{elec} \quad (3)$$

The total energy dissipated at the CH occurs at the following events; (1) When CH receive data from normal node, (2) When CH aggregates the received data (3) When CH sends the aggregated data to Base Station (BS). The total Energy dissipation at the CH is defined by equation (4).

$$E_{CH}=\left(\left(\frac{n}{m}-1\right)\times l\times E_{elec}\right)+\left(\alpha\times\frac{n}{m}\times l\times E_{AG}\right)+\left(\frac{\left(l\times E_{elec}\right)+\left(l\times\varepsilon_{fs}\times d_{BS}^2\right)}{\alpha}\right) \quad (4)$$

Where m is the number of clusters, is the processing cost of a bit per report to the BS and is the average distance between the CH and the BS, is the aggregation factor. The energy consumption for non-cluster nodes (CN) is represented by equation (5).

$$E_{CN}=l\times E_{elec}+l\times\varepsilon_{fs}\times d_{CH}^2 \quad (5)$$

Where, d_{CH} is the average distance between the CNs and their CH. Assuming the n nodes are uniformly distributed over an AxA square meter area and the distance between nodes and BS or between nodes and the CH is $\le d_0$, it can be shown by equation (6):

$$d_{CH}^2=\int_0^x\int_0^y\left(x^2+y^2\right).p(x,y)\ dx\ dy=\frac{A^2}{2\pi.m} \quad (6)$$

Where, $p(x, y)$ is the node distribution, and A is the network area. The energy dissipated in a cluster per round is given by equation (7).

$$E_C\approx E_{CH}+\left(\frac{n}{m}-1\right)\times E_{CN} \quad (7)$$

And the total energy dissipated in the network is estimated by equation (8).

$$E_T=\left(2\times n\times l\times E_{elec}\right)+\left(\alpha\times n\times l\times E_{AG}\right)+\left(\frac{l\times\varepsilon_{fs}\times\left(m\times d_{BS}^2+\left(n-m\right)\times d_{CH}^2\right)}{\alpha}\right) \quad (8)$$

In the proposed Cross-Layer IDS, the average number of CHs per round is $m=P_{\text{prob}}\times n$ during the life time of the network. This is a strict constraint the proposed Cross-Layer IDS maintains to ensure that the energy consumption is well distributed among the sensing nodes.

5.2 Experimental Setup

Multiple experiments with different running time were performed. Thirty test problems of different randomly generated durations were applied but, we notice that the results in all `experiments showed approximately the same behavior on the simulator. Consequently, we focused on three main experiments which actually repre-

sent the behavior of XLID system. Two types of detection methods were used, they are: non-cross-Layered IDS, and Cross-Layered IDS. At each experiment the concentration was on the number of detected attacks and the energy consumed at each method. Simulation time taken in the first experiment was 558.9 seconds, at the second experiment 427.5 seconds, and finally at third experiment is 394.7 s. A comparison was conducted between the methods regarding the number of detected attacks and the energy. Finally, analysis of the results was executed.

6. Results and Discussion

To start with, we quantified the number and level of assaults identified as the reenactment advances. We expect that assailant hubs target and assault arbitrarily organize hubs in the wake of being in uninvolved state (irregular day and age) and send each two-outline time a RTS bundle. Each packet has an ID and the packet may be in send, received, transmit, or collide state. Moreover, the packet when transmitted has start, transmit, and end states. In addition, the radio channel itself may be idle, reserved, or in requested state also. A clock tick when aggregated data are completed its transition, and a simulation time of about 600 s are performed. During the simulation a random packet are generated from both normal nodes and intruders' nodes. A special code was inserted in the intruder nodes packets to identify them from normal packets. The Energy consumption in joule through simulation time based on cross-layer compared to non-cross-layered detection methods clearly viewed in Figure 7. The number of detected attacks through simulation time based on cross-layer compared to non-cross-layered detection methods clearly viewed in Figure 8. We repeated the experiments on different simulation times to ensure that the proposed model is effective compared to others non-cross-layered methods. The second attempt of simulation was for 427.5s, and the third simulation experiment has been executed for a time of 394.7s.Table 2 summarizes the results of each detection method for both number of intruders, and total energy consumption. The number of attacks detected has been measured. We accept that aggressor hubs target and assault arbitrarily arrange hubs in the wake of being in inactive state (arbitrary era) and send each two-outline time an RTS bundle.

The second assessment step is to break down the conduct of XLID if there should be an occurrence of Sinkhole

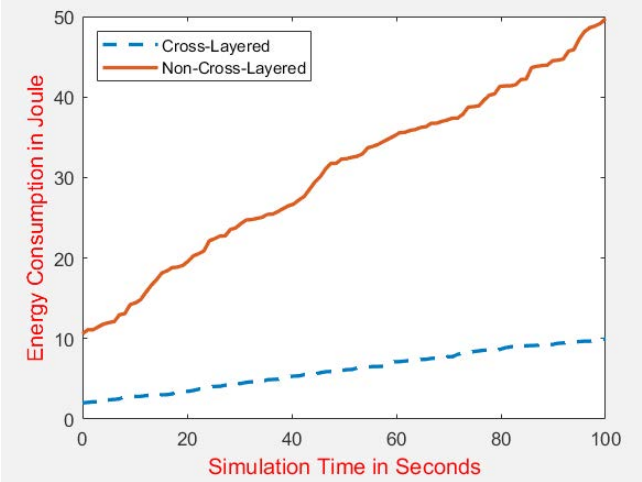

Figure 7. Energy Consumption of Cross-Layer and Non-Cross-Layered IDS.

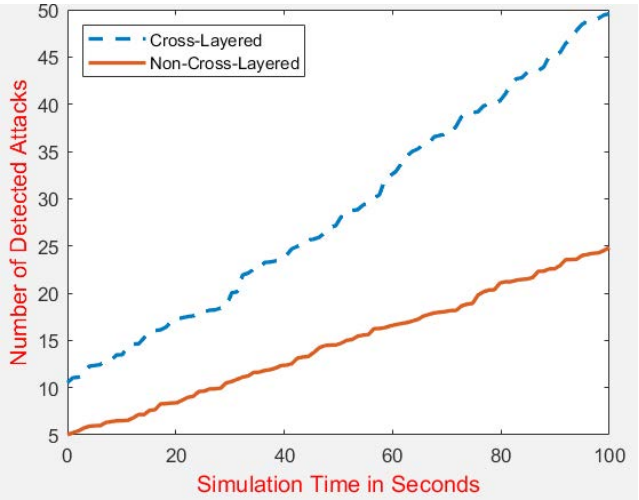

Figure 8. Number of Detected Attacks of Cross-Layer and Non-Cross-Layered IDS.

and specific directing assaults. For this, we gauged the aggregate of got messages by the base-station all through the reenactment time frame. Interloper hubs endeavor to make their assaults in irregular periods. In our reproduction, the gatecrasher hub which are nearest to the CHs endeavor to make a sinkhole to occupy a bigger information. Nonetheless, other gatecrasher hub (removed from CHs) perform particular steering assaults focusing on all hubs that are inside the scope of their radio Figure 9.

To assess the execution of XLID against assaults at the MAC layer, we directed a third reenactment in which the gatecrasher hubs perform assaults of depletion of vitality. We measure the aggregate vitality stores of the system

Table 2. Summary of Results for Each Method

Detection Method	Average Number of Detected Attacks in all Experiments	Average of Energy (in Joule) Consumption in all Experiments
Non-Cross-Layered	116	245
Cross-Layer	274	57

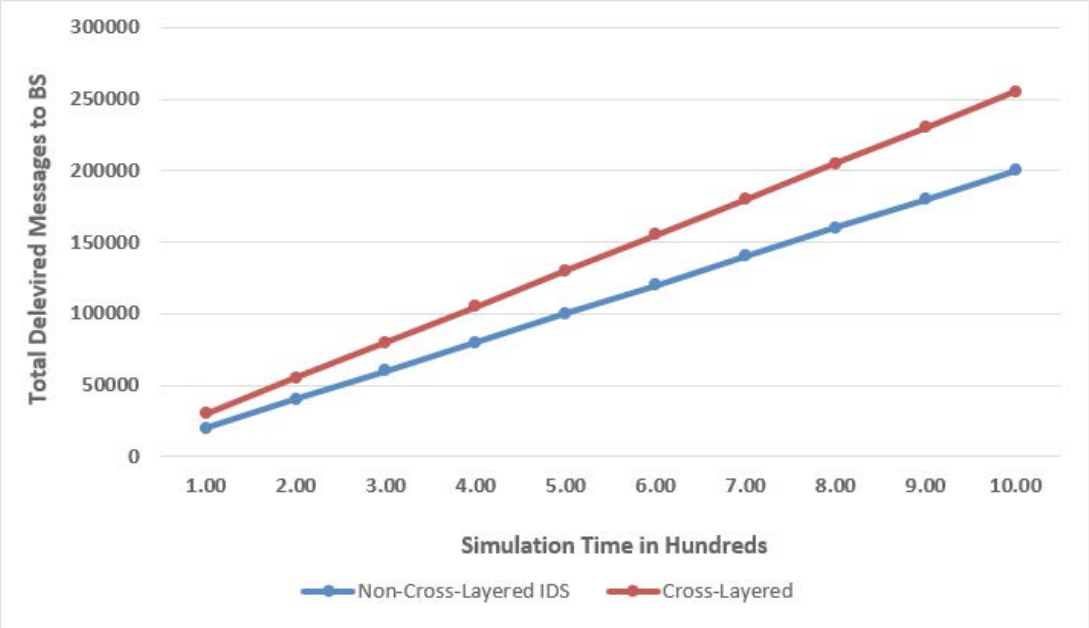

Figure 9. Number of Detected Attacks of Cross-Layer and Non-Cross-Layered IDS.

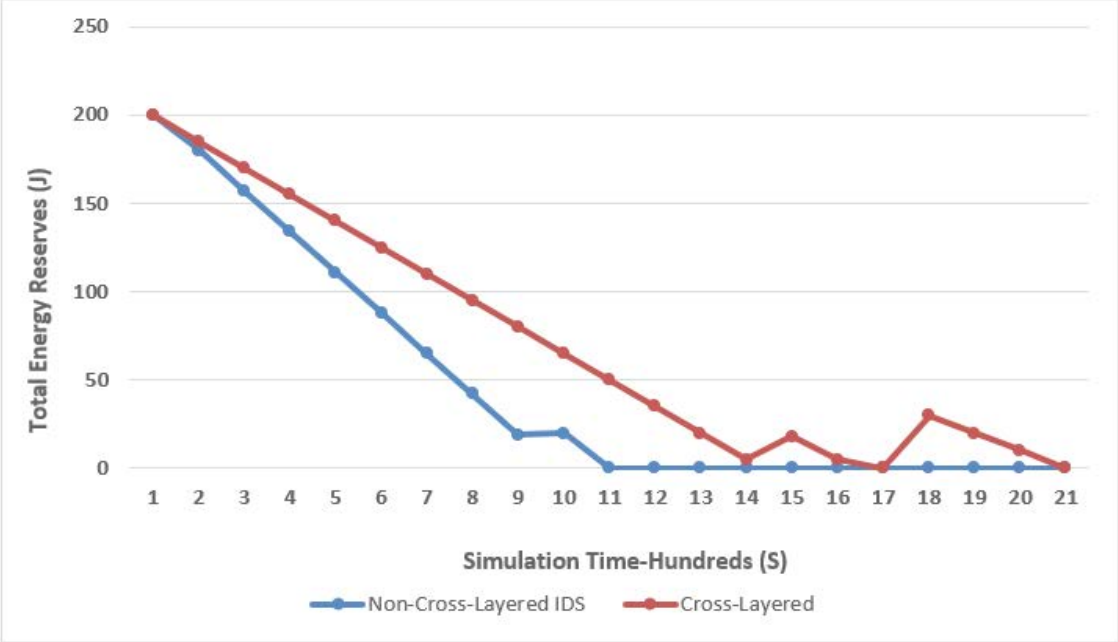

Figure 10. Total of energy reserves over the simulation time.

hubs also all through the reenactment time frame. Figure 10 demonstrates the outcomes. The graph in Figure 10plainly delineates the viability of XLID in forestalling assaults of vitality depletion at the MAC layer. With XLID, the sensor gatecrasher hubs expend their vitality holds frequently to transmit their gathered information. In any case, non-cross-layer IDS, the interloper hubs focused by the assaults exhaust rapidly their vitality saves, which specifically influence the system. Another important statistical information was extracted from the simulation shown in Figure 11.

7. Conclusion and Future Work

Wireless sensor Networks (WSNs) are especially defenseless against different assaults at various layers of the convention stack. Numerous interruption identification framework (IDS) have been proposed to anchor WSNs, yet a large portion of these frameworks work in a solitary layer of the OSI display. This, it is produced another interruption discovery show dependent on cross layer cooperation between system, and Mac OSI layers, called Cross-Layer IDS (XLID). This new XLID is checked and verified against other traditional IDS that are based on single layer protocol. For this purpose, a simulator was designed and implemented using MATLAB, especially for simulating the operational environment of the model. The proposed XLID showed its superiority in terms of number of detected attacks and power consumption over other single-layer based IDS. In this paper, we developed an XLID system for detecting Attacks early within the interaction between MAC and Network Layer. Then we compare our system to non-cross-layered IDS in terms of Energy consumption and number of detected attacks.

Findings proved that, XLID enhanced the attacks detection rate by 42%, which means that, when using XLID, we get higher detection rate for attacks by 42% compared to non-cross-layered IDS. Moreover, XLID shows 23% reduction in power consumption compared to non-cross-layered IDS.

Refereeing to throughput rate, we found that, XLID showed 75% increment in the messages throughput rate to base station compared to non-cross-layered IDS over the whole simulation time. In addition, by refereeing to percentage of energy saved during the simulation time in, XLID preserves from 25% up to 45% of energy compared to non-cross-layered IDS. It should be pointed out that the preserving energy depends on rate of attacks. During

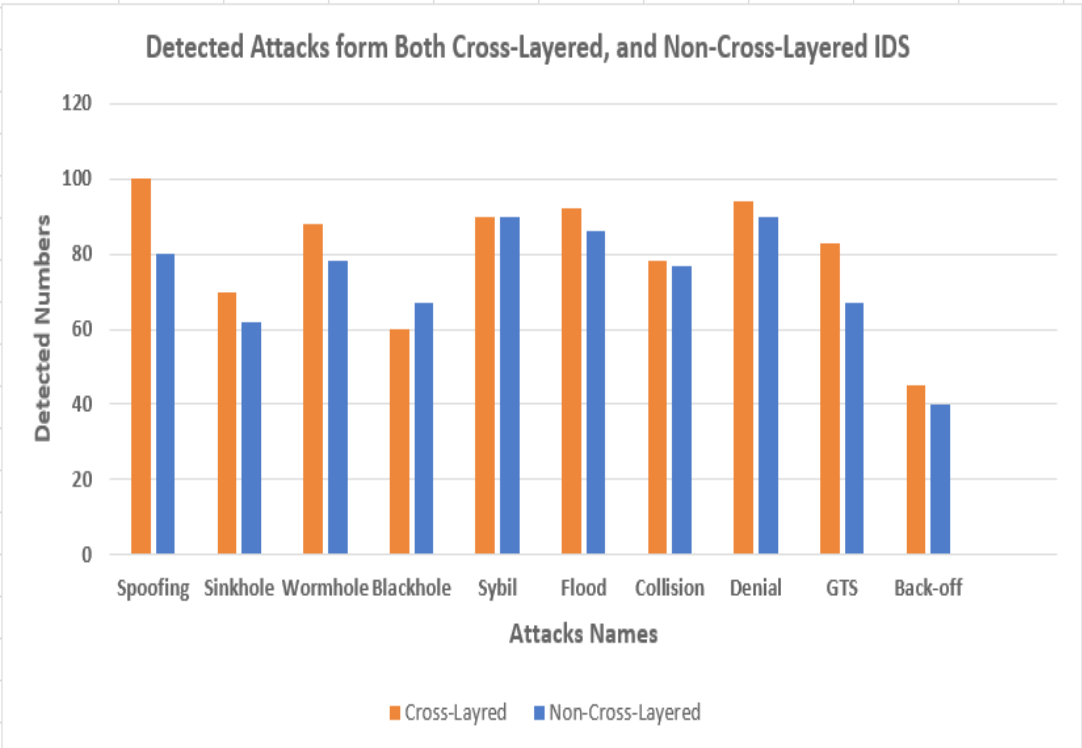

Figure 11. Attacks Detected by Cross, and Non-Cross IDS.

Table 3. Summary of the Results

XLID			Non-Cross-layered IDS		
Detection Rate Enhancement	Energy Enhancement	Throughput	Detection Rate Enhancement	Energy Enhancement	Throughput
Up to 42%	Up 25% up to 45%	Up to 75% higher than Non-cross-layered IDS	Less than XLID by 42%	It is always less than XLID by at least 25% up to 45%	Less than XLID by 75% at least
Attack Type Detection Rate			Attack Type Detection Rate		
• sybil, and collision attacks have the same rate of detection using non-cross-layered IDS • spoofing, sinkhole, wormhole, Denial, GTS, and Backoff get higher rate of detection using XLID by a range from 5% up to 20% • Blackhole attack is 5% lower in rate of detection compared to non-cross-layered IDS			• sybil, and collision attacks have the same rate of detection using XLID • spoofing, sinkhole, wormhole, Denial, GTS, and Backoff get lower rate of detection using non-cross-layered IDS. • Blackhole attack 5% higher in non-cross-layered IDS		
Layers Type			Layers Type		
Network Layer	Detection rate increased in this layer, it was from 5% up to 18% higher than non-cross-layered IDS except in Blackhole attack		Network Layer	Blackhole attack 5% higher than XLID	
MAC Layer	Higher than non-cross-layered IDS by the rate of 2% up to 15%, and for all MAC-Layer attacks		MAC Layer	Less than XLID for all MAC-Layer attacks	

the simulation, we studied the effect of targeted attacks, and target layers as presented. WE found that, both sybil, and collision attacks have the same rate of detection using XLID or non-cross-layered IDS. However, spoofing, sinkhole, wormhole, Denial, GTS, and Back off get higher rate of detection using XLID by a range from 5% up to 20% compared to non-cross-layered IDS. It is also noticed that, Blackhole attack violate the previous rule and it is 5% higher in non-cross-layered IDS compared to our XLID. Table 3 summarizes the above results of XLID against layered IDS.

The problem areas still existing in the proposed model providing new and future directions of research may aim at reducing the complexity while retaining the benefits of having multiple IDS working in a comprehensive manner to detect as well as resolve a novel attack scenario in WSNs. Moreover, it may also aim at optimizing the number of IDS to be considered for cross layer analysis in TCP/IP protocol while providing an effective security solution to handle novel attack types in WSNs. Still, the question has to be raised that if we can include more layers in our model and study the effect on IDS.

8. References

1. An Introduction to wireless sensor networks. Available from: http://ceng.usc.edu/~bkrishna/research/talks/WSN_Tutorial_Krishnamachari_ICISIP05.pdf. Date accessed: 2005.
2. Butun I, Morgera SD, Sankar R. Wireless Sensor Networks. International Journal of Distributed Sensor Networks. 2014; 16(1):266-82.
3. Mainwaring A, Culler D, Polastre J, Szewczyk R, Anderson J. Wireless Sensor Networks for Habitat Monitoring. Proceedings of the 1st International wireless sensor networks. 2002; p. 1-10. https://doi.org/10.1145/570738.570751
4. Puccinelli D, Haenggi M. Wireless sensor networks: applications and challenges of ubiquitous sensing. IEEE Circuits and Systems Magazine. 2005; 5:19-31. https://doi.org/10.1109/MCAS.2005.1507522
5. Xu G, Shen W, Wang X. Applications of wireless sensor networks in marine environment monitoring: a survey. Sensors (Basel). 2014; 14(9):16932-54. https://doi.org/10.3390/s140916932 PMid:25215942 PMCid:PMC4208207
6. Loo CE, Ng MY, Leckie C, Palaniswami M. Intrusion detection for routing attacks in sensor networks. International Journal of Distributed Sensor Networks. 2006; 2(4):313-32. https://doi.org/10.1080/15501320600692044
7. Wang Y, Chu W, Fields S, Heinemann C, Reiter Z. Detection of intelligent intruders in wireless sensor networks. Future Internet. 2016; 8(1):1-18. https://doi.org/10.3390/fi8010002
8. A Review on Security of Wireless Sensor Networks using Elliptic Curve Cryptography. Available from: https://www.researchgate.net/publication/260494836_A_Review_on_Security_of_Wireless_Sensor_Networks_using_Elliptic_Curve_Cryptography. Date accessed: 2014.

9. Silva APR, Martins MHT, Rocha BPS, Loureiro AAF, Ruiz LB, Wong HC. Decentralized intrusion detection in wireless sensor networks. 1st ACM International Work Qual Serv Security Wire l Mobile networks. 2005; p. 16-23.
10. Martynov D, Roman J, Vaidya S, Fu H. An Intrusion Detection System for Wireless Sensor Networks. Techniques. 2007; 3:507-12.
11. Bhuse V, Gupta A. Anomaly Intrusion Detection in Wireless Sensor Networks. Journal of High Speed Networks. 2005; 15(1):33-51.
12. Rajaram A, Palaniswami S. A Trust Based Cross Layer Security Protocol for Mobile Ad hoc Networks. Journal of Computer Science. 2009; 6(1):165-72.
13. Alrajeh NA, Khan S, Shams B. Intrusion Detection Systems in Wireless Sensor Networks: A Review. International Journal of Distributed Sensor Networks. 2013; 4:1-7. https://doi.org/10.1155/2013/167575
14. Boubiche D, Bilami A. Cross Layer Intrusion Detection System for wireless sensor network. International Journal of Network Security & Its Applications. 2012; 4(2):1-18. https://doi.org/10.5121/ijnsa.2012.4203
15. Su WT, Chang KM, Kuo YH. eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks. 2010 International Conference on Electronics and Information Engineering. 2007; 51(4):1151-68.
16. Towards intrusion detection in wireless sensor networks. Available from: https://www.researchgate.net/publication/228340105_Towards_intrusion_detection_in_wireless_sensor_networks. Date accessed: 2007.
17. Krontiris I, Dimitriou T, Giannetsos T, Mpasoukos M. Intrusion detection of sinkhole attacks in wireless sensor networks. Algorithmic Aspects of Wireless Sensor Networks. 2007; p. 150-61.
18. Liu F, Cheng X, Chen D. Insider Attacker Detection in Wireless Sensor Networks. Proceedings of the IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications. 2007; p. 1937-45. https://doi.org/10.1109/INFCOM.2007.225
19. Yu Z, Tsai JJP. A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks. 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2008; p. 272-9. https://doi.org/10.1109/SUTC.2008.39 PMCid:PMC2604134
20. Coppolino L, Romano L. Open Issues in IDS Design for Wireless Biomedical Sensor Networks BT - Intelligent Interactive Multimedia Systems and Services. Smart Innovation, Systems and Technologies. 2010; 6:231-40. https://doi.org/10.1007/978-3-642-14619-0_22
21. Hai TH, Huh E, Jo M. A lightweight intrusion detection framework for wireless sensor networks. Framework. 2010; p. 559-72. PMid:20427620
22. Kaur D, Singh P. Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack. ACEEE International Journal of Network Security. 2014; 5(1):1-6.
23. Ozel O, Tutuncuoglu K, Ulukus S, Yener A. Fundamental limits of energy harvesting communications. IEEE Communications Magazine. 2015; 53(4):126-32. https://doi.org/10.1109/MCOM.2015.7081085
24. Wang K, Stolfo SJ. Anomalous Payload-Based Network Intrusion Detection. International Workshop on Recent Advances in Intrusion Detection. 2004; p. 203-22. https://doi.org/10.1007/978-3-540-30143-1_11
25. Revathi S, A. M. A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. International Journal of Engineering Research and Technology. 2013; 2(12):1848-53.