A Low-Power Detection System for Wireless Sensor Networks

Ardalan Forootaninia
Dept of IT, Tehran University, Kish International Campus
Kish, Iran
Forootaninia@ut.ac.ir

M. B. Ghaznavi-Ghoushchi *member IEEE*
School of Engineering, Shahed University
Tehran, Iran
Ghaznavi@shahed.ac.ir

***Abstract*—Wireless networks are increasingly spanning the globe and so the security and privacy of these networks are of great importance. Sensor networks have their own vulnerabilities so, preventing intrusions and detecting them has become one of the most challenging issues. In this paper, we propose an approach to implement a hierarchical intrusion detection system. In this model, the network is divided into smaller units called cells and the intrusion detection program is installed on each cell representative. The main purpose to present this model is to reduce the power consumption as a key factor for increasing the lifetime of sensor nodes. In addition, an improved watchdog technique is proposed for detecting malicious nodes. This technique resolves common problems in watchdog mechanism. The proposed hierarchical model has been implemented in Tiny-OS environment and the results indicate that, our proposed model is better in performance than the original models and it has increased the lifetime of the wireless sensor nodes by around 5370 seconds for a network with 200 sensors.**

Keywords—Wireless Sensor Networks, Intrusion Detection System, Hierarchical IDS, Watchdog, Low-Power, Sensor life time.

I. INTRODUCTION

Intruding into a network refers to any activity which endangers the integrity, confidentiality and accessibility of a source and an Intrusion Detection System (IDS) is a system which detects Intrusion activities [1]. The main idea of developing intrusion detection systems came from examining the behavior patterns of ordinary users and identifying the abnormal behavior patterns of the users. An IDS which operates statistically demonstrates the network traffic like radar and detects any signal which may indicate an abnormal event or attack to the network [2].

So far, different techniques have been proposed for intrusion detection in wireless sensor networks (WSNs). In the following sections some of them are discussed.

In [3] and [4] a new technique has been proposed for identity authentication in wireless sensor networks in an interleaved manner which is called Interleaved Hop-By-Hop authentication (IHOP). IHOP guarantees to indentify all incorrect packets injected into the network. In the method [3], the wireless sensors networks are organized hierarchically and in clusters. The cluster in upper hierarchy creates a route for connection to base station and each interface node reaches a node connected to its upper level and also a node connected to its lower level. In IHOP an upper cluster collects the information related to identity authentication from its members (subordinates) and sends it to the base station in form of a report. This reporting occurs only when at least 1+t sensor observes similar results. This paper does not show how the t parameter should be adjusted to sensor network. However, IHOP guarantees that the base station will identify the incorrect packets (when more than t nodes did not agree to cooperate).

Another method [4] proposed route filtering using statistical methods which can identify and delete incorrect data. In this method, there is a key extensive pool and each sensor is allocated a part of this pool. Whenever a move in the region begins, the sensors identify this move and one of the nodes as the base station checks all the network addresses and filters all the reports en route conveying the address incorrectness. However, as mentioned in [5], this method is used for protecting the network against incorrect information injection and cannot drive away the attacks such as selective forwarding.

Also, another approach [6] was proposed based on a routing called INSESN (Intrusion-Tolerant Routing in Wireless Sensor Networks) in which the sensors collect the information related to regional typology and send it to the base station. Afterwards, the base station creates the routing table according to the collected information and sends it to the related sensors. The base station is the main control point for creating the routing table which reduces the nodes computational load. Although INSENS has been developed by a protocol based on routing table, these are base stations which collect all the information and create the routing table for each sensor. However, INSENS is not suitable for large sensor networks [6].

During the recent years, intrusion detection based on the statistical techniques has been widely under the spotlight. For example [7], uses data analysis techniques (such as clustering and neural networks [8]) using the data available

in the user's reports, has examined and predicted their behavioral algorithm and tried to optimize the efficiency of intrusion detection in the system and separate abnormal algorithms from the normal ones using various presumptions and the intelligent technology.

In wireless networks battery life of the node plays an important role because it is very difficult to recharge battery regularly [9] so in view of these works, in this paper we propose an approach for implementing new intrusion detection system to increase the network's lifetime and security level. The proposed algorithm solved the following known problems: impartial removal, selecting the incorrect malicious node, limited power transfer, and node conspiracy.

The remainder of this paper is organized as follows. Section II provides existing vulnerabilities of WSNs. Our proposed algorithm is discussed in section III. The mathematical model for estimating networks lifetime is given in section IV and the Tiny-OS simulation will be explained in section V. Experimental results are given in section VI and section VII concludes the paper.

II. VULNERABILITIES

The vulnerabilities in network cause attack occurrence. If we succeed to minimize them, we can contribute to increase the level of security in the network. In fact, the vulnerabilities are the only controllable parts in wireless sensor networks. As a result of these natural limitations in WSNs, Denial Of Service(DOS) attacks which can cause damage to sensor networks by consuming the energy and the available sources [10] are the main power consumption attacks. Table I indicates DOS attacks and the vulnerable points which cause attack occurrence.

According to the basic need of security attacks in WSN can be categorized:

- Collision, selective forwarding and flooding attacks which affect network availability.
- Tampering, sinkhole which can threaten confidentiality.
- Misdirecting, Wormhole, Sybil attacks which can affect packet integrity.
- Collision, Jamming, Sinkhole and Hello message which affects communication.

TABLE I DENIAL OF SERVICE ATTACKS

Attacks	Description
Jamming attack	Jamming attack occurs as a result of intentional interference in the radio waves in order to prevent a node from using radio channel [10].
Tampering attack	Most of the professional attackers are able to intrude into the nodes memory and get access to the information inside or the encoding keys. Also, they can replace the programs and codes with malicious ones [12].
Collision attack	In these attacks, like jamming attacks, the attacker identifies the wireless exchanges around the victim node and creates Collision and destroys the key packets [13].
Interrogation and Exhaustion attack	An attacker can create DOS attacks by inserting the nodes to his message re-sending [13].
Selective forwarding attacks	In wireless sensor networks, all the nodes can participate in routing operation to find the best route for sending the message. Only one node may not deny sending the packet and advertizing a specific route for its neighbors. This can sometimes create black holes in routing [13], [14].
Misdirecting attack	An attacker can misdirect the network nodes by sending the messages to wrong routes [15].
Sinkhole attacks	In the attacks so-called sinkhole attacks, the attacker uses the traffic in the sensor network as a prey for intruder's infiltration [15].
Wormhole attacks	In these attacks, the route advertisers cooperate to be able to create a lateral channel for communication (the result of several attacker's cooperation) [16].
Sybil attacks	Most of the used protocols for the network nodes assume a unique ID. However, the attacker node in Sybil attacks has several IDs [17].
Flooding Attack	Flooding attack covers and use the victim`s limited sources such as memory, processing cycle and band width [18].
Hello Message Flooding	Since many protocols creates neighboring tables though exchanging Hello messages, these attacks cause various disorders in the system such as increasing the traffic in radio channels and decreasing the nodes operational power [18].

III. INTRUSION DETECTION SYSTEM

A. *Basic Watchdog*

The watchdog in WSN [11] is malicious nodes detection algorithm which is based on the broadcast property in the networks. In this case, A which sends a packet to C, can eavesdrop the sent traffic of B and determine whether or not B will send the packet to C (Fig. 1).

B. *Modified Watchdog*

In this paper, we proposed a power-aware IDS algorithm based on the improvement of watchdog mechanism.

In figure 2, i is the buffer counter, P_A is the packet sent by the node A, P_{BC} is the sent packet from B to C, t is the maximum waiting time and $b(i)$ is the content of cell i in buffer M.

In the proposed modified watchdog algorithm, for a given WSN with three specific nodes of A, C, and cluster node M, if node A starts to send a message to node C, the cluster head node (M) operates as a watchdog. In this case, the cluster node starts to send a warning message to the upper layer for any additional task or operation or warning. If the number of alerts or warnings reaches a specific limit, the cluster head node introduces B as a malicious node.

C. Basic tasks flowchart

The basic tasks flow of the handled operations for intrusion detection is shown in figure 3 in order to facilitate understanding the proposed technique. The steps of the algorithm for detecting malicious nodes are as follow:

Algorithm 1 Detecting Malicious Nodes

1) A sends a packet to C via B. meanwhile, M (the cluster head node) eavesdrops the packet saves a copy in its counterpart section in buffer b.
2) The node M eavesdrops to the communication between B and C for t second (this time depends on the nodes processing and sending speed as well as the sensors type) and refers to the step 5 in the case of not receiving any packet.
3) The F_i value is calculated if M hears the P_{BC}.
4) If F_i=0, the message in cell *bi* (where its counterpart message has been saved in buffer b) will be deleted and the algorithm moves to the step 6. If $F_i \neq 0$, the message remains in the buffer and moves to step 5.
5) The warning message, signaling the maliciousness of the node B, is sent to the upper layer by the cluster head node.
6) The end of the algorithm

D. Rule Based Hierarchical Model

We propose a model for saving the power consumed by the nodes while implementing an intrusion detection system in wireless sensor networks. As shown in figure 4, this model follows a hierarchical architecture. The whole system is divided into smaller parts (called cells). Each cell indicates the sensory limit of a node and the node is called cluster head node. It must be emphasized that, unlike the conventional IDS models like [19], our proposed algorithm does not necessarily require arranging the sensors in the system in order. This means, the number of the sensors in the cells can be flexible. The system topology may be altered. In the proposed algorithm, the fixed nodes in the network are limited to the regional and cluster head nodes only. These nodes should be selected at the outset of designing the network by the base station.

1) The intrusion detection entities

a) Cluster Head Nodes

These nodes are responsible for monitoring the related region. These nodes eavesdrop to the data sent by the nodes

Fig. 1. Basic Watchdog Mechanism

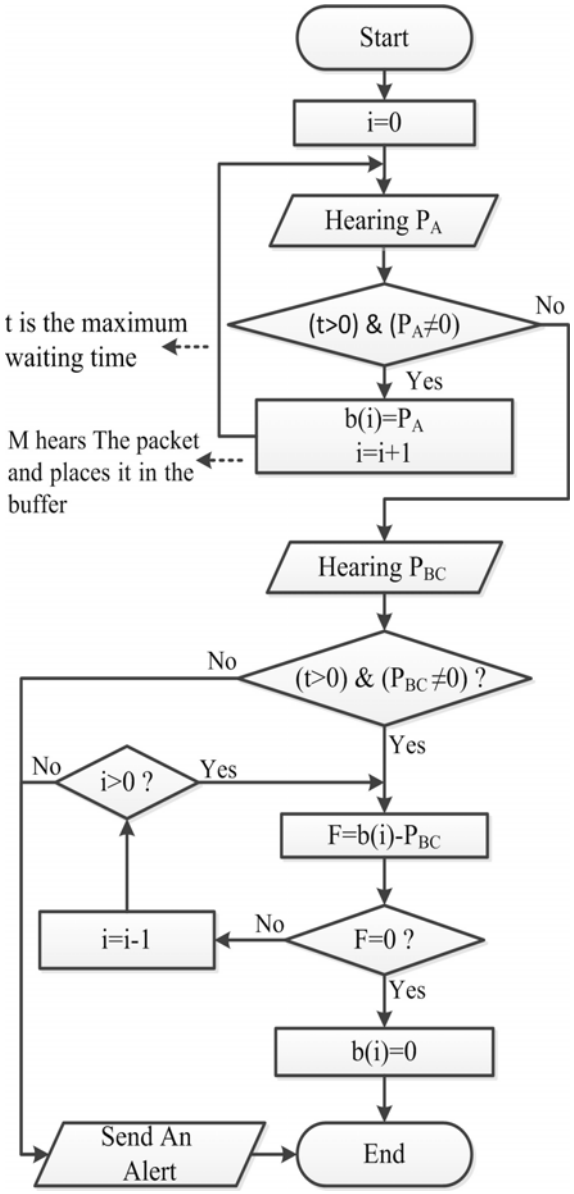

Fig. 2. The Proposed algorithm for intrusion detection in WSNs

under their control, analyze the data and inform their upper nodes (local nodes) of the suspicious cases. In fact, compared to the other sensors, these nodes enjoy more capacities including the intrusion detection program installed on them.

b) Local node

These nodes are in charge of controlling and receiving the information from their neighboring cluster head nodes

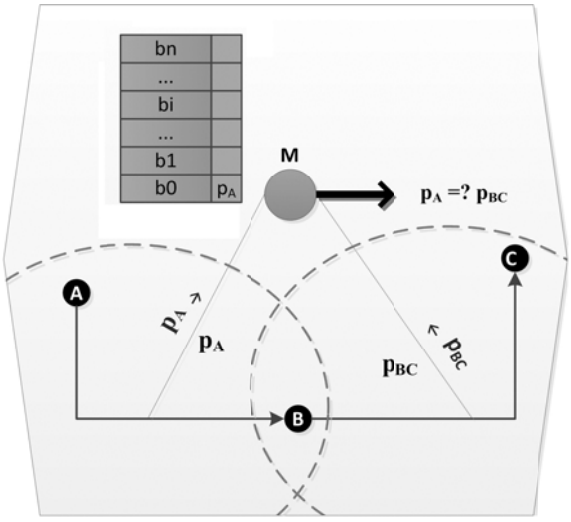

Fig. 3. Modified Watchdog Mechanism

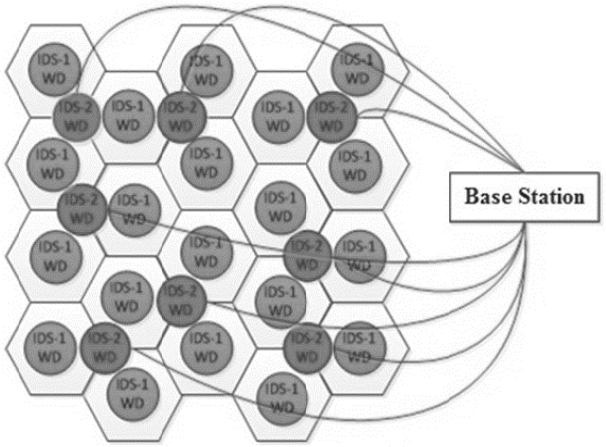

Fig. 4. Watchdog nodes in the proposed model

as well as sending warning message to the upper layer which is the base station. These nodes have all the abilities of the intrusion detection system. In addition, they allow integration into larger networks. Therefore, even in presence of a large number of sensors, the network can be divided into smaller section to be easily manageable.

c) Base Station

The base station is the top level of the proposed model which is directly supported by human force. This station receives the information from the local nodes, analyzes them and applies the necessary operations and policies to the system.

E. Instructions to implement the hierarchical IDS

1) The number of Cluster Head Nodes (Layer 3)

In the second part, we should select low-level cluster heads. The number of cluster head nodes (layer 2), for three layers network architecture can be calculated by: (n is the number of nodes)

$$\left\lfloor \frac{n}{Max\_Nodes\_Each\_Cells} \right\rfloor + 1 \qquad (1)$$

2) The number of Local nodes (Layer 2)

Since we assume three-layer architecture, first we should select the high-level cluster head nodes then the low-level ones. The number of cluster head nodes (layer 3), for three layers network architecture can be calculated by:

$$\left\lfloor \frac{\left\lfloor \frac{n}{Max\_Nodes\_Each\_cells} \right\rfloor + 1}{Max\_nodes\_Each\_cells - 1} \right\rfloor + 1 \qquad (2)$$

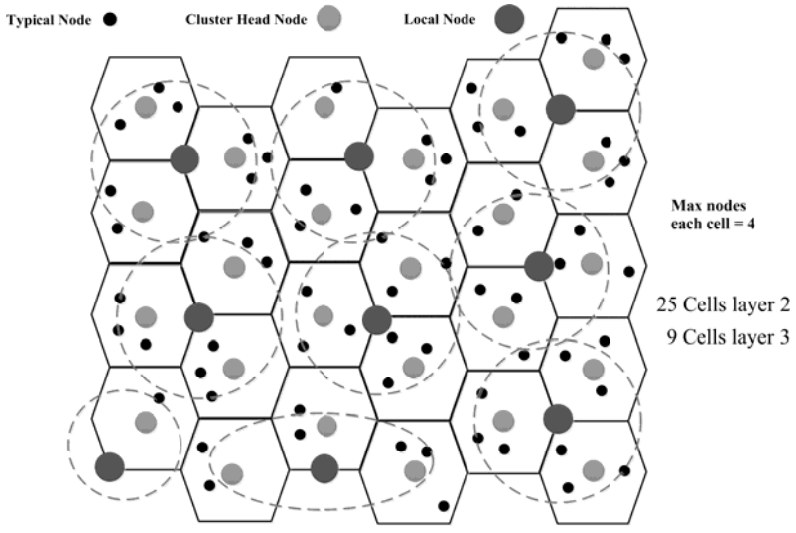

Fig. 5. A Sample Design for a network (max nodes each cell = 4, n = 100)

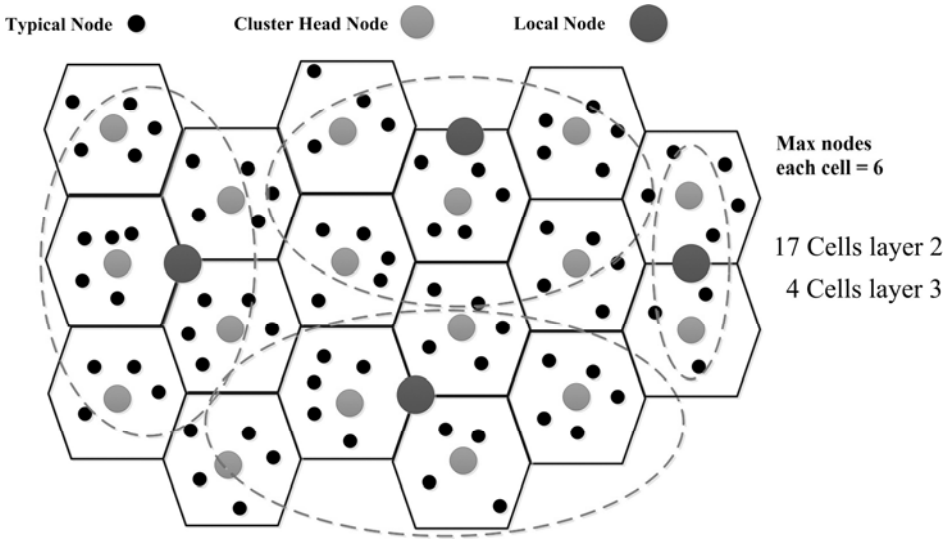

Fig. 6. A Sample Design for a network (max nodes each cell = 6, n = 100)

3) Cluster Head and Local Nodes Selection

Cluster head nodes are selected according to their life period. The cluster head node life should not be less than a specific time. We call it, **threshold life period**. This duration is different for each cluster head node due to the lower level nodes and It equals to the longest life period among the low-level sensors of a cluster head node.

4) Implementing IDSs

The intrusion detection programs can be only implemented on cluster head nodes or each cell representative. Therefore, the power consumed by the intrusion detection program should be also taken into the account in implementation process. Because some of the primary energy of the cluster head node *i* is consumed for implementing the intrusion detection system while booting. Each cell indicates the sensory limit of a node. Two Sample Designs regarding the proposed instruction have been shown in Fig. 5 and Fig. 6.

IV. Mathematical Model for Estimating Lifetime

Power in the examined wireless sensor network can be obtained through computational techniques. Moreover, power as a desirable feature can prolong the life of sensor nodes and the network [20].

Generally, the largest portion of the sensors power in wireless sensor network is used for receiving and sending the information. Therefore, here the main focus is on energy consumption for receiving and sending the information in the functional points of the wireless sensor network (such as the nodes containing IDS). The minimum power consumed $P_t(d)$ for sending 1 bit of information at Euclidean distance d (and P_r is the minimum power consumed for receiving 1 bit [20]:

$$P_t(d) = a_1 + a_2(d)^n \tag{3}$$

$$P_r = B \tag{4}$$

Where a_1 the parameter related to sender circuit , equals 50 nj/bit , a_2 parameter related to sender booster, equals 100 Pj/bit/m^2, d stands for the distance between the functional point *i* and the target functional point, and *n* refers to the parameter related to the local emission reduction which equals 2. *B* refers to the parameters related to receiver circuit which is 50 nj/bit. Power consumption in a single node in time unit is calculated according to the equation 3 [20].

$$e_{it} = r_{ri}\, P_r + (r_{ri} + r_{gi})\, P_s \tag{5}$$

Where r_{ri} refers to the produced information bit rate in the functional node i. r_{gi} refers to the produced information bit rate in the node i and P_s is minimum power consumed for sending information which is equal with $P_t(d)$. With regard to the fact that raw information bit rate in wireless sensor network is considerably low compared to the other common wireless network, the high quality of the information and fast transfer is not of high importance. The average speed of raw information production is 512 bps which is evidently very low in some applications. The life period of the each functional point *i* equals to primary energy ratio to energy consumption in time unit. This is shown in the equation below [20]:

$$L_i = \frac{e_i}{e_{it}} \tag{6}$$

Where e_i refers to the primary energy of the functional node *i* which is calculated according to:

$$e_i = R\, I^2\, t \tag{7}$$

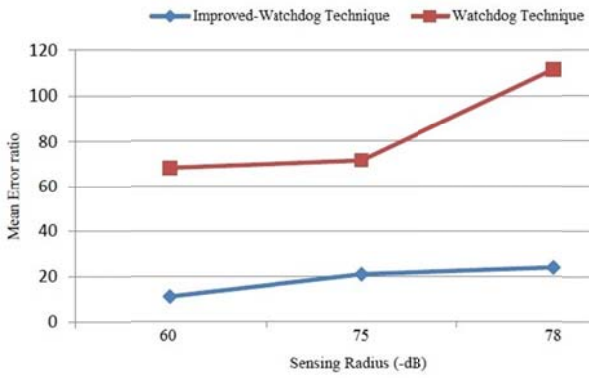

Fig. 7. Error ratio versus sensing radius

According to [21], R stands for resistance which considered 1 ohm and I, is 8 mA for an active node, and t is the node's boot time.

For more details about the equations refer to [20], [21].

V. Simulation and Experimental Results

In this paper, Tiny-OS environment has been used for our simulation that runs in the Linux operating system. TOSSIM [22], [23] is a Tiny-OS mote SIMulator which is useful for testing both the algorithms and implementations; however it does not simulate the physical phenomena that are sensed [24]. Instead of compiling one of the Tiny-OS programs in each components of wireless sensor network, users can use TOSSIM which can be run in PCs. Furthermore, it should be taken into the account that TOSSIM, primarily aims at providing a simple and high-level simulation for Tiny-OS programs. We have used NesC for coding. NesC is a programming language designed to facilitate the structuring concepts and execution model of Tiny-OS. It is an extension of C which guarantees the code will be efficient on the target microcontrollers that are used in sensor networks [25], [26].

The Sensor network simulating has been conducted assuming 200 sensor nodes. The simulation results show the simulated network follows the theoretical pattern. This argues "the more the distance, the more the power consumptions". Moreover, it shows a similar behavior. So, increasing the distance between nodes and the base station increases the cost (energy per unit tasks) on send and receive tasks and hence consumes the node energy and remaining power. However, it must be noticed that other factors including primary energy of the nodes, the node's sleeping cycle and the intrusion detection system are also affecting on energy reduction too.

In the first part of our experiments, we tried to set various sensing radiuses. The results are shown in figure 7. It is clear that, when we limit monitoring only to nodes with stronger signal, mean error ratio is lower.

As it can be seen, the improved watchdog technique has less error than the original watchdog technique and it seems to be more efficient. The highest mean error rates are within the -78 dB which is about 23 for improved watchdog and 111 for watchdog. According to our results, it appears that, the -60 dB is more appropriate. It has to be mentioned that, for comparing the network lifetimes between two models and normalizing the nodes, we assume that the intrusion detection program has been already installed and implemented on all nodes.

Table II, shows the comparison between watchdog and improved watchdog techniques. As you can see, four problems of watchdog techniques have been resolves in the improved technique.

In the second part of our experiment, we proposed a hierarchical model; as it mentioned, the intrusion detection program can be implemented only on the cluster head and the local nodes (not on the other nodes). However, in the normal model, it can be implemented on all nodes and each node conducts the intrusion detection operation separately and each node operates as a cluster head node.

Figure 8 shows nodes lifetime differences in the proposed and the normal model. As the chart indicates, the biggest lifetime difference belongs to node 119 which means, node 119 lives 60.17136 seconds more than its counterpart node (in the normal model). Similarly, the other nodes are also indicated. It can be concluded that the proposed model has enhanced the network lifetime approximately by 5370 seconds. However, it is to be mentioned that in some nodes (e.g. node 15), the lifetime has not been increased.

Thus, in the proposed model, less energy is consumed for implementing the intrusion detection program. As a whole, in this model, 3488.976 mJ less energy was consumed compared to the normal model. This energy value is considerable for some wireless sensor network applications.

As figure 9 shows, 25 % of nodes increased lifetimes were between 0 to 6.01 seconds. 7 % of them were between 24.07 to 30.09 seconds and 42 % were between 30.09 to 36.10 seconds. Also, 17.5 % of nodes lifetimes were increased between 36.10 to 42.12 seconds, 7 % of them were increased between about 42.12 to 48.14 seconds, 1 % of nodes increased lifetimes were between 48.14 to 54.15 second and at last, 0.5 % of their lifetimes were increased between about 42.12 to 48.14 seconds.

Finally, we simulated three networks which were included 50, 100 & 200 nodes. After implementation of the proposed model, we have calculated the Lifetimes of nodes, the overall network Lifetimes with implementing the proposed model in compare to the normal model have been shown in figure 10. As a result, there has been a rapid growth when the number of nodes increases.

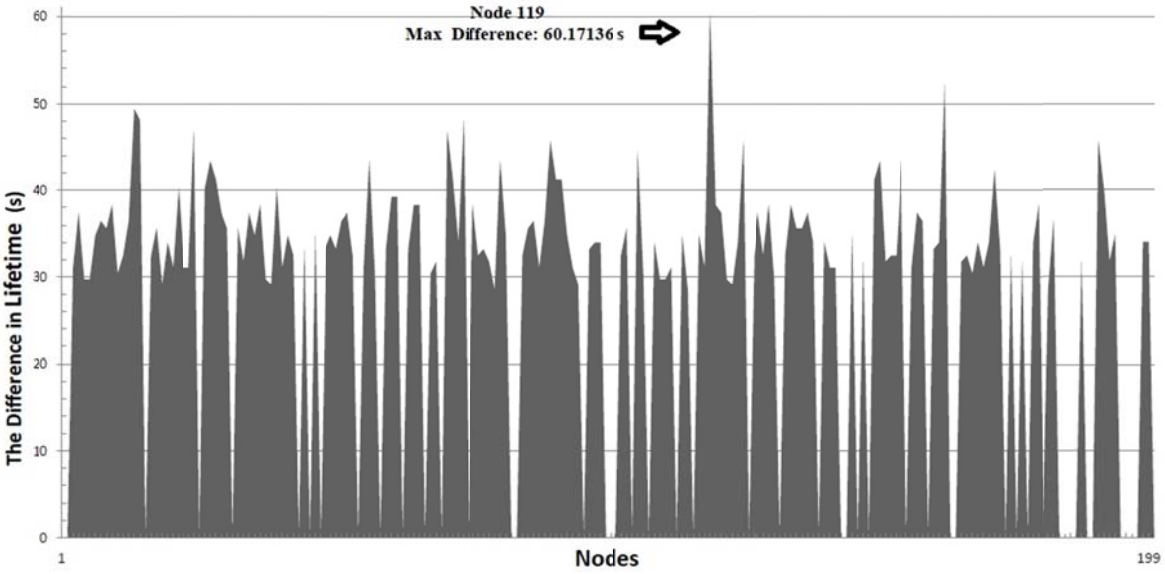

Fig. 8. Node's Lifetime differences between the proposed and the normal models for a network with 200 nodes

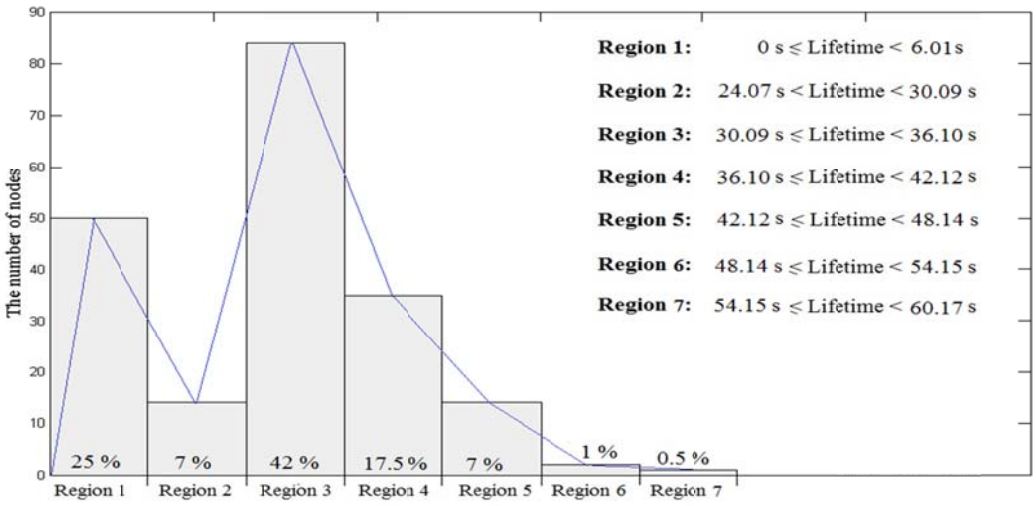

Fig. 9. Lifetimes increased regions by implementing the proposed model for a network with 200 nodes

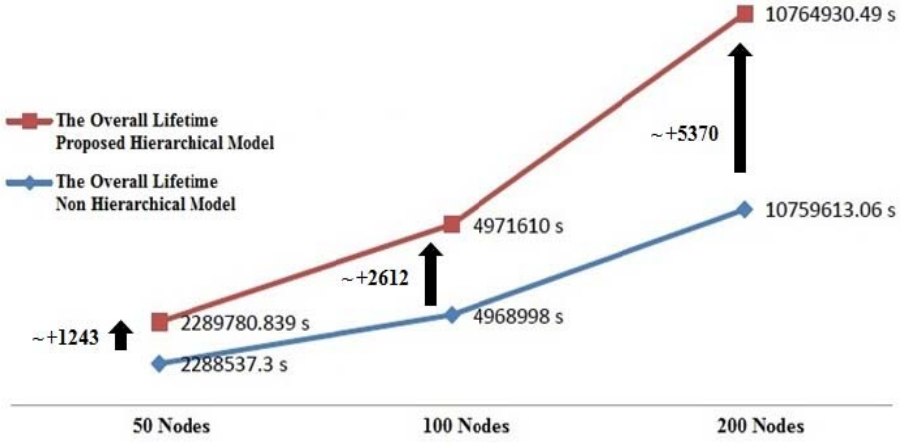

Fig. 10. Node's Lifetime differences between the proposed and the normal models

TABLE II THE COMPARISON OF IMPROVED WATCHDOG WITH WATCHDOG

Problems	Watchdog	Improved Watchdog
Impartial removal	Yes	No
Collision in the receiver	Yes	Yes
Selecting the incorrect malicious node	Yes	No
Limited power transfer	Yes	No
Node conspiracy	Yes	No
Creating ambiguous Collision	Yes	Yes

VI. CONCLUSION AND FUTURE WORKS

Wireless sensor Networks are widely used in many applications spanning from industry to research areas. One of the major limitations in the WSN is the limited power sources
for the nodes. The life of the network in many situations is directly related the life of its power sources. There are various attacks on the WSN targeting the power consumption of the network with dummy tasks and activations to alleviate the life and functionality. In this paper, a new modified watchdog algorithm is proposed to prolong the sensor nodes (and the network) Lifetime. The proposed algorithm is a new hierarchical architecture over the conventional limitations on the fixed positions for network nodes. The fixed nodes in the network are limited to the regional and cluster heads only.

Overall, in the proposed model less energy is consumed for implementing the intrusion detection program. As figure 10 shows, our model would be very useful for wide networks with too many nodes.

The implementation has been conducted on a sensor network simulated in Tiny-OS. The results indicate that, with implementing our model we can increase the lifetime up to +1243 seconds for a network with 50 nodes, +2612 seconds for a network with 100 nodes and about +5370 seconds for a network with 200 nodes.

In addition, the conclusions pertaining to the hierarchical model are as follows:

- Network design based on layering technique enables the other sensors in a cell to cover the related region if the energy of one or more sensors ends. As a result, the sensor network operation will continue without encountering any problem.
- Hierarchical design increases the network security. Because, if there is a malicious node in each layer, both the upper layer and the nodes in the same layer will detect it. Therefore, here the node maliciousness can be detected in two ways. Moreover, since the local nodes are directly monitored by base station, they are not likely to be intruded.
- Monitoring the layered networks is much more convenient. Because in the layered networks only the last layer nodes are monitored and the other nodes are managed by this layer. However, in the other networks, we are generally forced to be in touch with a wider range of nodes.

Wireless sensor networks needs an intrusion detection system which operates regionally distributed. This system should be economical in terms of communications, energy and memory [27].

As stated in [28], IDS trends are shifting from host based IDS to network based IDS, and from centralized IDS to distributed IDS. Moreover, the trends are towards having IDSs that are resistant to attacks and interoperate with other IDSs in heterogeneous environments.

So far, many studies have been carried out on establishing and preserving security and intrusion detection in wireless networks (such as wireless sensor networks). The research areas can be included as principles, intrusion detection techniques, collecting information, reacting against attacks, IDS architectures, testing, and IDS security.

Some of the studies mentioned above, have been reached an acceptable step and most of them have been conducted on intrusion detection techniques.

REFERENCES

[1] S. Şen, John A. Clark, Juan E. Tapiador, "Power-aware intrusion detection in mobile ad hoc networks," *Ad hoc networks*, 2010, pp. 224-239.

[2] Y. Wang, *Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection*, Idea Group Inc (IGI), 2008.

[3] S. Zhu, S. Setia, S. Jajodia, P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 3, 2007, pp. 1-32.

[4] F. Ye, H. Luo, S. Lu, L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, 2005, pp. 839-850.

[5] Y. Zhang and H. Hu, *Security in wireless mesh networks*: Auerbach Publications, 2008

[6] J. Deng*l*, R. Han, S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, 2006, pp. 216-230.

[7] M. Khalilian, N. Mustapha, M. Sulaiman, A. Mamat, "Intrusion Detection System with Data Mining Approach: A Review," *Global Journal of Computer Science and Technology*, vol. 11, Issue 5, Version 1, 2011, pp. 1-7.

[8] B. Shah and B. H. Trivedi, "Artificial Neural Network based Intrusion Detection System: A Survey," *International Journal of Computer Applications*, vol. 39, no. 6, 2012, pp. 13-18.

[9] TN. Nagabhushan, S.P.Shiva Prakash, K. Krinkin, "Minimum Battery Draining Rate Aware Optimized Link State Routing in Wireless Mesh Networks," *13th FRUCT conference*, Russia, April 2013, pp 111- 120.

[10] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems,* pp. 739-763, 2004.

[11] M. J. Kim, M. Medard, J. Barros, "Algebraic watchdog: mitigating misbehavior in wireless network coding," *Selected Areas in Communications, IEEE Journal on,* vol. 29, 2011, pp. 1916-1925.

[12] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," *In Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, Oakland, California, November 1996, pp. 1-11.

[13] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review,* vol. 5, 2001, pp. 11-25.

[14] S. Cheung and K. N. Levitt, "Protecting routing infrastructures from denial of service using cooperative intrusion detection," *Security Paradigms Workshop UK*, 1998, pp. 94-106.

[15] M. S. I. Mamun and A. F. M. S. Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network," *International Journal of Network Security & Its Applications (IJNSA),* vol. 2, no. 3, 2010, pp. 102-117.

[16] K. Nasr, AA. El Kalam, C. Fraboul, "Generating Representative Attack Test Cases for Evaluating and Testing Wireless Intrusion Detection Systems," *International Journal of Network Security & Its Applications (IJNSA),* vol. 4, no 3, 2012, pp. 1-19.

[17] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," *In Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, Oakland, California, November 1996, pp. 1-11.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks,* vol. 1, 2003, pp. 293-315.

[19] M. S. I. Mamun and A. F. M. S. Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network,"*International Journal of Network Security & Its Applications (IJNSA),* vol. 2, 2010, pp. 102-117.

[20] V. Gholampour, "Optimizing power consumption in wireless sensor network", M.A. thesis, Department of Computer and Electrical Engineering, Tehran University, 2003.

[21] Harvard University: UCB Mica2 Mote Power Benchmark Summary Web: http://www.eecs.harvard.edu/~shnayder/ptossim/mica2bench/summary.html.

[22] A. Pandey and R. Tripathi, "A Survey on Wireless Sensor Networks Security," *International Journal of Computer Applications IJCA,* vol. 3, 2010, pp. 43-49.

[23] S. Krit, J. Laassiri, S. El. Hajji, "Modeling and Simulation Methodology Techniques for Advanced Low Power Communication Circuits," *Lecture Notes in Engineering and Computer Science,* vol. 2192, 2011.

[24] A. Dwivedi and O. Vyas, "An Exploratory Study of Experimental Tools for Wireless Sensor Networks," *Wireless Sensor Network,* vol. 3, 2011, pp. 215-240.

[25] M. Bokare and M. A. Ralegaonkar, "Wireless Sensor Network: A Promising Approach for Distributed Sensing Tasks," *Excel Journal of Engineering Technology and Management Science*, vol. 1,2012, pp.1-9.

[26] B. L. Honus, "Design, implementation and simulation of intrusion detection system for wireless sensor networks," Master Thesis, MASARYKOVA University, 2009.

[27] A. Giannetsos, "Intrusion detection in wireless sensor networks," Master Thesis, Carnegie Mellon University, 2009.

[28] S. Sen, "Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks," PhD Thesis, Department of Computer Science, University of York, 2010.