Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 9 (2014) pp. 034-042

A Central Mechanism to Protect Wireless Sensor Network from External Attacks

Hosam Soleman[1] and Ali Payandeh[2]
[1] Department of ICT Maleke-Ashtar University Islamic Republic of Iran
hjss_11975@yahoo.com
[2] Department of ICT Maleke-Ashtar University Islamic Republic of Iran

***Abstract*- Because of the widespread use of wireless sensor networks in many applications, and due to the nature of the specifications of these networks (WSN) in terms of wireless communication, the network contract specifications, and published it in difficult environments. All this leads to the network exposure to many types of external attacks. Therefore, the protection of these networks from external attacks is considered the one of the most important researches at this time. In this paper we investigated the security in wireless sensor networks, Limitations of WSN, Characteristic Values for some types of attacks, and have been providing protection mechanism capable of detecting and protecting wireless sensor networks from a wide range of attacks.**

***Keywords*:** Wireless Sensor Network (WSN), Attack, protection mechanism, Packet flow, Security, abnormal.

I. Introduction

The wireless sensor networks are used in many potential applications nowadays, such as, temperature monitoring, light monitoring , and monitoring a battle field to detecting enemy's movement, monitoring the battle field.. etc. These networks consist of thousands of nodes-sensitive, where these nodes are deployed in open environments and non-protected, leading to the exposure of the network to the many dangers and external attacks. [1].
The main characteristics of WSNs are low energy use, dynamic and self-organizing operations, mobility of nodes, dynamic network topology, communication loss, heterogeneity of a nodes and scalability to large scale of deployment, ease of use. Wireless sensor networks can be used for many critical applications such as target tracking in battlefields and emergency response. The main goal of WSNs is to make longer the life time of network [2], tolerate sensor damage, and battery power. In WSNs energy is mainly consumed for following purpose: data processing, signal processing and hardware operation. The main challenges in WSNs are decreasing the sensor size and cost.
There are several mechanisms, theories and algorithms presented in this domain, but did not achieve full protection of the network from these attacks and intrusions. Therefore, it is necessary to find more mechanisms and techniques evolved to protect the network from a wide range of attacks.

We proposed in this paper an autonomic mechanism to detect attacks in wireless sensor networks (WSN) by taking advantage of the effects that occur in the network when exposing to external attacks. All attacks affect the network features that are: incoming packets, outgoing packets, neighbors, Sending Packet Interval, RTS Packet Arrival Rate, the strong of received signal, and collisions related to each node.

II. Security in WSN

Wireless sensor nodes network means that shares common property as computer network. So we need security issues: - Attack and Attacker: - Attack means that unauthorized person access to a service. For security we need secure resource or information we need integrity, availability, or confidentiality of a system. Attackers can create fault and weakness in a security design, implementation, configuration or limitation are occurs.

A. Authentication

WSNs transfer information and sensitive data for different important decision making. Receiver wants to the data with ensure that are correct source for decision-making process [3]. Authentication provides ensure to sender node and receiver that data is secure in which they want to communicate.

B. Integrity

Integrity means ensure that there must no tampering and extra data. Receiver check that data received is exactly

original and same as send by the sender. Data integrity is to ensure that information is same during transmission by using some security key for ensure [3].

C. Confidentiality

It gives guarantee that data send by the sender will not access by attacker. Encryption key is used for sending the message. Confidentiality means create security from unauthorized parties and attacker.

D. Scalability

Scalability means that no node compromise and no increase communication when size of network is grow. It should allow nodes to be added in network with proper deployment as well [4].

E. Self-Organization

In WSN every sensor node is in dependent and flexible enough to be self-organizing in different environments. No fixed infrastructure is available for WSN Network management. In self-organizing we used conduct key management. In self-organization we used conduct key management and building trust relation among sensor for security [3].

III. Limitations of WSN and attacks on WS

1. Data transmission rate and lifetime of sensor network can be limit due to interference among the transmission and limited energy source of the sensor. In WSN limitation occurs that in care of security design and deployment in sensor network. Difficult to develop proper security that balances demanding security performance against sensor node. In Hostile Environment, the nodes can't be safe from physical attack, anyone can access to the location where they are deployed. Physical attacker used this sensitive information for illegal purpose [4].
2. Random Topology: Random distribution used by a sensor network in a remote environment. Design various encryptions among a group of neighbours. Difficult to design key agreement that are not require certain nodes to be neighbours of some other nodes [4].
3. Sensor Energy: Limited energy supply in each sensor node that can create a problem in data transmission rate and the lifetime energy source of the sensor. Processor and sensor energy are usually less important unless the node has a powerful processor executing large programs [4].
4. Ad-Hoc Deployment: Sensor nodes are not need any infrastructure they work on randomly monitoring field. Sensor nodes itself create connections with other nodes and make on infrastructure. Hence we need new protocol should be able to handle this ad-hoc deployment [5].
5. Fault Tolerance: Sensor nodes fail due to energy exhaustion and unattended environment. One sensor node is fail effect on all sensor networks because sensor node is need to maintain connectivity and prolong lifetime of network [5].
6. Communication and environmental: WSN consist of a collection of tiny sensor nodes having made of wireless communication. Internal and External attacks are creating insecure nature of wireless communication channels. Insufficient speed of communication disturbs the propagation of wave and hack your networking [6].
7. Expensive: High power consumption requires regular battery changes so costly**.**

IV. Attacks on WS

Because the specifications for wireless sensor networks, which have been described above, these networks are exposed to a lot of attacks. In this paragraph will explain some of these attacks [18], which will be used to influence the network to assess our central mechanism.

- **Black holes (sink holes):**
  It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.
- **Flooding:**
  Flooding also occurs at the network layer. An adversary constantly sends requests for connection establishment to the selected node. To hit each request, some resources are allocated to the adversary by the targeted node. This may result into effusion of the memory and energy resources of the node being bombarded.
- **Sybil Attack:**
  This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as disparity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, and topology maintenance and misbehavior detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node.
- **Selective Forwarding:**
  Selective forwarding is a network layer attack. In this, an adversary covenants a node, that it scrupulously forwards some messages and plunge the others. This hampers the quality of service in WSN. If the attacker will drop all the packets then the adjoining nodes will become conscious and may evaluate it to be a flaw. To avoid this, the attacker smartly forwards the selective data. To figure out this type of attack is a very tedious job.
- **Worm holes:**
  In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. A wormhole is a low-latency junction between two sections of a network. The malicious node receives

packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

- **Hello Flood Attacks:**
  Hello flood attack uses HELLO message to advertise itself to its adjoining nodes and a node receiving this message may consider that it is within radio vicinity of the sensor. In this type of attack, an adversary with a high radio transmission range and processing power sends HELLO message to a number of sensor nodes which are scattered in a large area within a WSN. It gives an illusion that the malicious node is their neighbor. When the assured nodes will send message to the base station, then it passes through the malicious node as this node provides the shortest route to the base station as an illusion. When the information reaches the attacker, the victim is betrayed by it. This leads to data congestion and thus complicates the data flow in the network.
- **Acknowledgement Spoofing:**
  Acknowledgements play a significant role in certifying the quality of service and creating another links. Acknowledgement spoofing attack is introduced on routing algorithms at the network layer that needs transmission of acknowledgement messages. An attacker may eavesdrop packet transference from its adjoining nodes and swindle the acknowledgements, thereby sending wrong information to the nodes.
- **Collision**
  Collision is a type of link layer jamming that occurs when two nodes try to transfer data at the same time and at the same frequency. An attacker may cause collisions in particular packets such as ACK control messages. The effected packets are transmitted again, increasing the energy and time cost for transmission. Such an attack reduces the network perfection.
- **Exhaustion**
  Exhaustion occurs at the link layer. This attack dominates the power resources of the nodes by causing them to retransmit the message even when there is no collision or late collision.
- **Unfairness**
  MAC protocols at link layer administer the communications in networks by constraining priority schemes for seamless correlation. It is possible to use these protocols thus affecting the precedence schemes, which ultimately results in decrease in service.

V. Relevant knowledge

Detection Mechanisms refer to the continuous monitoring of the network or system when they are in operational case, Detect attacks that violate the security policy, detect abnormal behavior, vandalism malignant, in addition to those mechanisms do defensive work against these attacks [7]. Basing on many detection mechanisms, the detection mechanisms can be classified for two types:

1- Anomaly detection: In this category, the system or network must be establishing normal behavior and saving that information about normal behavior in secure database, in order to use it to discover abnormal behavior. The famous researches in this area are: based on Statistics[8], Cluster[9], Data Mining, Immunization Methods[12], Multi-agents[10], Neural Network, Support Vector Machine(SVM) [11],Hidden Markov Model [13].

2- Misuse detection: in this category the protection mechanism attempting to identify instances of network attacks by comparing current activity against the expected actions of an intruder. In this type of mechanisms, the technique of mechanism based on expert system, State Transition Analysis, Model Reasoning, Pattern Matching techniques etc.

In [14] in this work they proposed a method Randomized and Trust based witness finding strategy for replication attack detection mechanisms in wireless sensor networks (RTRADP) with trust factor. Resilient to malicious witness and increasing detection rate by avoiding malicious witness selection.

In [15 in this paper they had presented some counter measures against the sinkhole attack.

In [16] they proposed a machine learning solution for anomaly detection along with the feature extraction process that tries to detect temporal and spatial inconsistencies in the sequences of sensed values and the routing paths used to forward these values to the base station. And they proposed a way to integrate mobile nodes in the approach, which is the main novelty of this work.

VI. Protection mechanism

Protection mechanism depends on detecting the abnormal behavior. The network topology that has been used is a cluster topology, as shown in Figure 1.

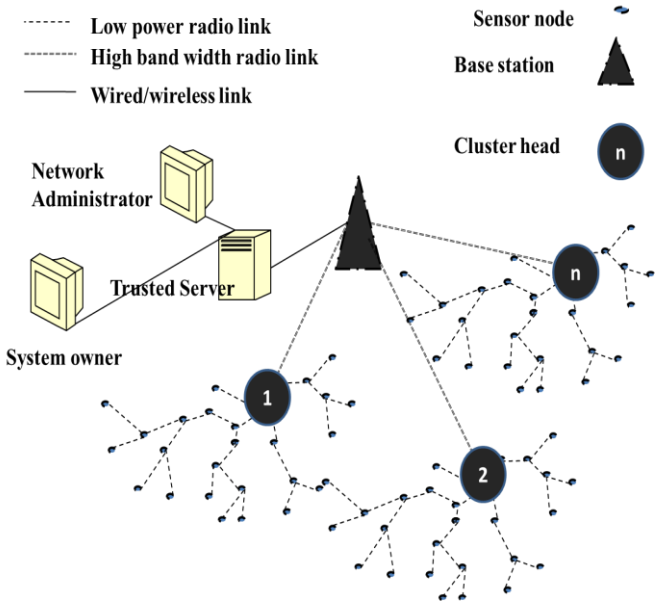


Figure.1: Clustering of wireless sensor networks diagram

Some important considerations must be clarified and that are:

1. The protection mechanism located in base station.

2. All the heads of clusters send their data directly to the base station.
3. Each node in the cluster must send its data only to the cluster head of this cluster.
4. The base station has this attributes: safe, large resources and it can communicate with each cluster head node. The proposed protection mechanism can protect network from the:
   - Known attacks (Abnormal behavior resulting from these attacks is known), such as, Collision Attacks, Unfair Competition, Exhaustion Attacks, Selective Forwarding, Sinkhole, Sybil, Wormhole, and Hello Flood.
   - Unknown attacks (Abnormal behavior resulting from these attacks is unknown): Because the work of mechanism includes Self-learning phase, as will explain later.

The work of mechanism similar to work of the brain, the brain receives data from all body and detects the abnormal behavior depending on the inherent data that stored in the brain and the other acquired data. As shown in figure 2.

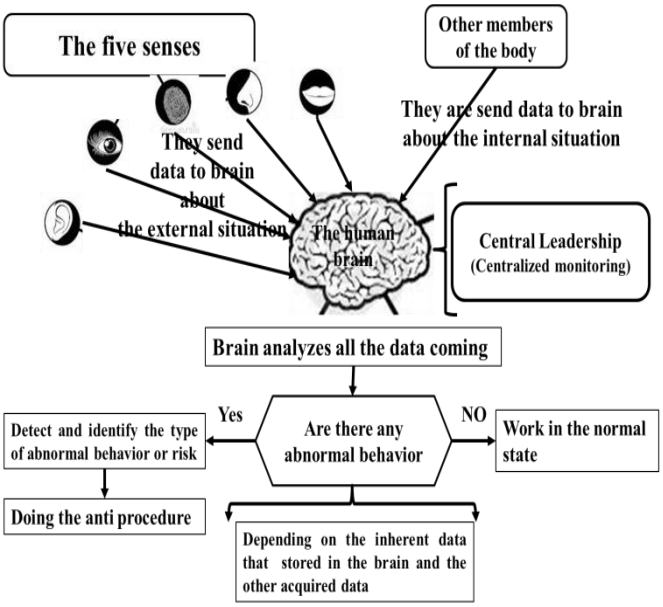


Figure.2: Detecting the abnormal behavior by the brain

Figure 3 shows the work diagram. The protection system consists of four phases:

1. Data Collection and Pretreatment

In the natural state of the network, the mechanism builds database containing the characteristics of the network when operating in the natural state without the presence of any attack. These data bases contain information such as: Packet Delivery Waiting Time, Packet Collision Ratio, Average Time of Sending Packet Interval, RTS Packet Arrival Rate, Packet Drop Ratio, Neighbor Count, and Packet Delivery Signal Strength, etc. In this phase, the average value is calculated for each of the above corresponding characteristic, and during a specific time period (t).

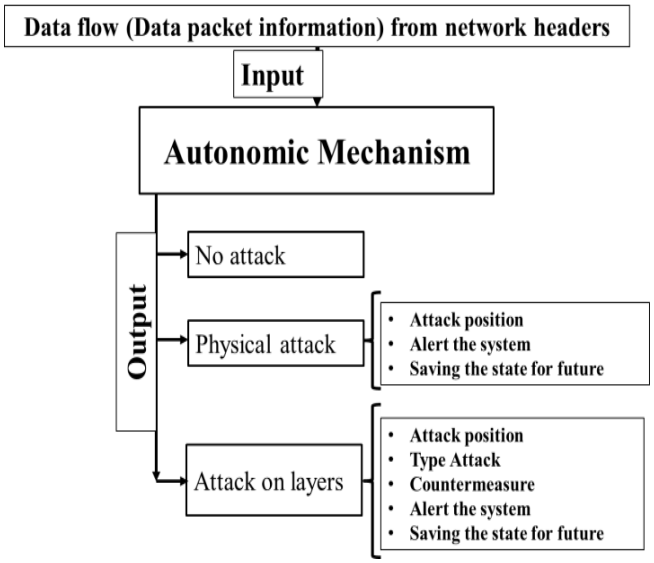


Figure.3: Work diagram

Figure 4: shows the A central protection mechanism.

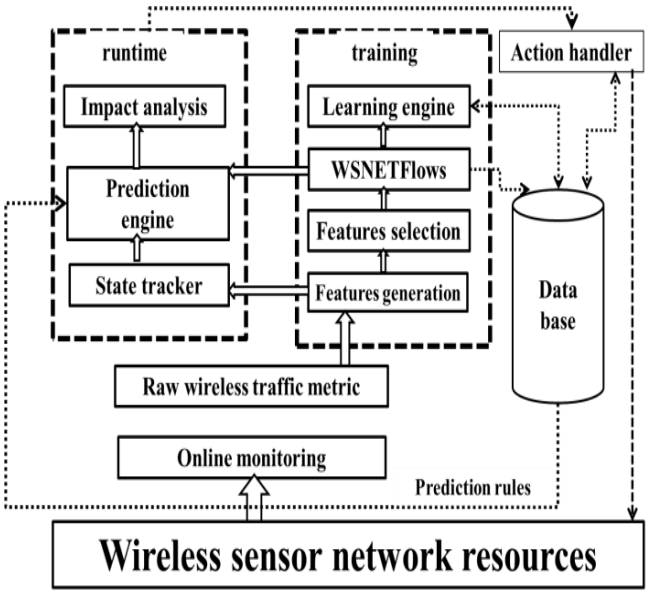


Figure.4: Central protection mechanism

At the end of this phase, we obtain the following table 1 and table 2 and table 3, and At the end of this phase the mechanism creates backup for these data to be used when it need it.

Table 1

Cluster heads IDs	**Packet Delivery Waiting Time**	**Packet Collision Ratio**	**Average Time of Sending Packet Interval**	**RTS Packet Arrival Rate**	**Packet Drop Ratio**	**Packet Delivery ratio**
ID1						
ID2						
ID3						
.						
.						
IDr						

Table 2

Network Nodes	***Count of neighbors***
Node0_ID	
Node1_ID	
Node2_ID	
.	
Noden_ID	

Table 3

Network Nodes	***Packet Delivery Signal Strength***
Node0_ID	
Node1_ID	
Node2_ID	
.	
Noden_ID	

2. Attack Detection

In this phase: the work of the mechanism is divided into specific time periods, during each period, the algorithm tests one of the data stored in the data base.

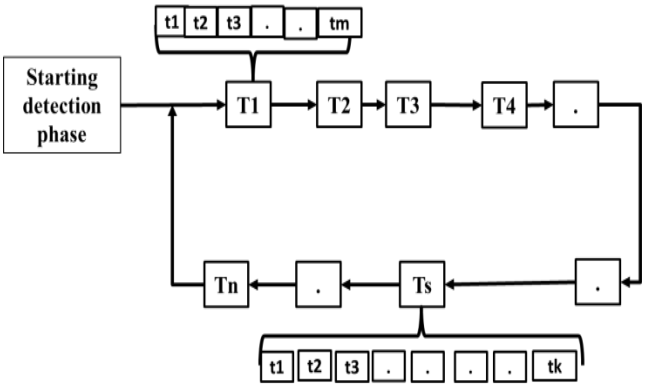
In this phase of the work of mechanism is split into equal time periods (T1, T2, ... , Tn), the number of that periods equal to the number of corresponding characteristic that were collected in the first phase (in this work n=8). Each time period (Ti) allocate to test one corresponding characteristic. For example: during T3 the mechanism tests the Packet Drop Ratio.

Each time period (Ti) is split into equal time periods (t1, t2, ..., tm), where m the number of cluster heads in the network. (Note: ti in this phase is equal to t in Data Collection phase). During ti mechanism calculate the average value for corresponding characteristic for specific cluster head.

Ti that responsible to test the Packet Delivery Signal Strength and Ts that responsible to test the Count of neighbors are divided to k time periods, where k is the number of sensor nodes in the network.

When detection an abnormal behavior, the algorithm transforming to attack response phase.

Upon completion of all tests, the mechanism return to the starting point and re-testing of the new (in this phase of the algorithm continues its work continuously, intervention in closed loop, as shown in the figure 5)



- n: number of corresponding characteristic
- m: number of cluster heads
- k: number of sensor nodes

Figure.5: attack detection phase

3. attack Response

In this phase:

- The base station sends message to all nodes in that region, message commands all the nodes in that region by choosing different work, Depending on the type of attack detected. for example:
  when the mechanism detect worm hole attack, the base station sends message to all nodes in that region, message commands all the nodes in that region by choosing different path for each sending.
- Alerting the system administrator.

4. Self-learning phase

In this phase, when the protection system finds abnormal behavior and there is no prior information about this behavior, the network protection system alerts existence of an attack and tells the system administrator, and records data for this attack to be used in the future if the network have been attacked from attack that causes such this abnormal behavior.

VII. Evaluation protection system (ANOMALY - BASED Autonomic Mechanism):

In order to evaluate the mechanism has been used:

True Positive (TP): This occurs when an IDS raises true alerts on a detected malicious traffic. Hence TP is the total detected malicious activity.

True Negative (TN): This occurs when there's no malicious activity taking place in the network, and the Intrusion Detection system is thus not raising any alarm. Hence TN can be obtained by subtracting TP from the total monitored traffic.

False Positive (FP): This occurs when an IDS erroneously raises a false alarm over a legitimate activity in the network. These can be generated from adapting the IDS to a normal non-malicious traffic [20].

False Negative (FN): This occurs when the IDS fails to detect a malicious activity taking place in the network.

False Positive Rate (FPR): This shows the proportion of instances which were not an intrusion, but were still alerted on. FPR is obtained using the following formula:

$$FPR = \frac{FP}{FP + TN}$$

True Positive Rate (TPR): This rate shows how good the IDS is at detecting intrusions in a network. It is also called the Detection Rate. TPR is obtained as:

$$TPR = \frac{TP}{TP + FTN}$$

Positive predictive value: ratio of true positives to combined true and false positives, which is as much a statement about the proportion of actual positives in the population being tested as it is about the test. Positive predictive value is obtained as:

$$\textbf{Positive predictive value} = \frac{TP}{TP+FP}$$

Negative predictive value is obtained as:

$$\textbf{Negative predictive value} = \frac{TP}{TP+FP}$$

Figure 6 shows the relationships among above terms

		Autonomic mechanism conditions (rules-based)		
		Condition Positive	**Condition Negative**	
Test Outcome	**Test Outcome Positive**	**True Positive**	**False Positive (Type I error)**	**Positive predictive value = Σ True Positive / Σ Test Outcome Positive**
	Test Outcome Negative	**False Negative (Type II error)**	**True Negative**	**Negative predictive value = Σ True Negative / Σ Test Outcome Negative**
		***positive rate* = Σ True Positive / Σ Condition Positive**	**true negative rate = Σ True Negative / Σ Condition Negative**	

Figure.6: Relationships among terms

Detection rate: It is quantified as the probability that a certain protection system can detect a certain wireless sensor attacks. The detection rate (DR) is computed as the percentage of times a certain attack type is detected when attacks from the same type are launched n times as given in Equation 1:

$$\boldsymbol{DR_j = \sum_{i=1}^{n} \frac{N_{i,j}}{n}} \quad , \boldsymbol{N = \{0, 1\}} \qquad \text{Equation 1}$$

Where n is the total number of variations for attack type j; N(i,j) is 1 if the attack is detected and 0 if the attack is not detected. The total detection rate measures the wideness of detection for a certain protection system.

VIII. Simulation results

a. Simulation parameters:

Ns-2 simulator will be used to evaluation mechanism [17]. The table 4 shows the simulation parameters:

Table 4. Simulation parameters

channel type	Wireless Channel
radio-propagation model	Propagation/Two Ray Ground
network interface type	Phy/Wireless Phy/802_15_4
MAC type	Mac/802_15_4
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/Omni Antenna
max packet in ifq	100
number of sensor nodes	80
protocol type	AODV
X dimension of topography	500 m
Y dimension of topography	500 m
simulation period	500 second
Energy Model	Energy Model
value	Initial energy 100
number of CH (cluster head) nodes	8
number of base station node	1

We run this simulation for many times and detected different commonly attacks. We have successfully detected maximum abnormal events. Using this model we calculate the percentage of abnormal events. The simulation result was shown in Table5.

Table 5. Detection rate

Type	Percentage(%) of detection rate for								
	CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8	Avg≈
Collision Attacks.	97.2	94.85	93.8	98.3	96.9	95.5	93.7	97.8	96%
Unfair Competition.	92.2	94.85	93.8	94.3	91.9	95.5	93.2	96.8	94%
Exhaustion Attacks	89.2	91.85	91.8	89.3	87.4	95.5	92.98	88.8	90%
Selective Forwarding,	88.2	93.85	91.8	93.3	91.4	94.5	92.4	91.8	92%
Sybil	97.12	98.67	98.8	97.34	97.13	99.4	98.51	98.23	98%
Sinkhole.	91.98	90.85	93.8	94.76	95.9	95.5	95.88	95.8	94%
Wormhole	93.88	95.5	97.2	97.8	98.3	94.23	96.9	95.8	96%
Hello Flood.	92.2	94.85	93.8	94.3	91.9	95.5	93.2	96.8	94%

The results shown in Table 6 show the values of TN, TP, FN, FP, TPR, and FPR.

Table 6: Protection system Performance evaluation through 530 rate instances

Type	TN	TP	FN	FP	TPR	FPR
Hello Flood.	530	43	3	2	93.48%	0.38%
Collision Attacks.	530	56	4	3	93.33%	0.56%
Unfair Competition.	530	39	2	1	95.12%	0.19%
Exhaustion Attacks	530	40	3	2	93.02%	0.38%
Selective Forwarding,	530	55	3	2	94.83%	0.38%
Sybil	530	50	5	3	90.91%	0.56%
Sinkhole.	530	31	3	1	91.18%	0.19%
Wormhole	530	52	4	1	92.86%	0.19%

The result shows that the mechanism performs optimally.

1- False positive rate of less than 1% in all cases.
2- High true positive rate depicting an effective performance.
3- Average detection rate of more than 90%.

Self-learning:

As explained previously, the mechanism includes a number of stages, one of that stages is the self-learning phase, it means any attack on the network (abnormal behavior in the network) The system can be detected and added to the data as an attack is unknown, and alert the system administrator. The system administrator gives the name for that attack depending on previous information or other information.
The figure 7 shows the diagram of mechanism work in this phase.

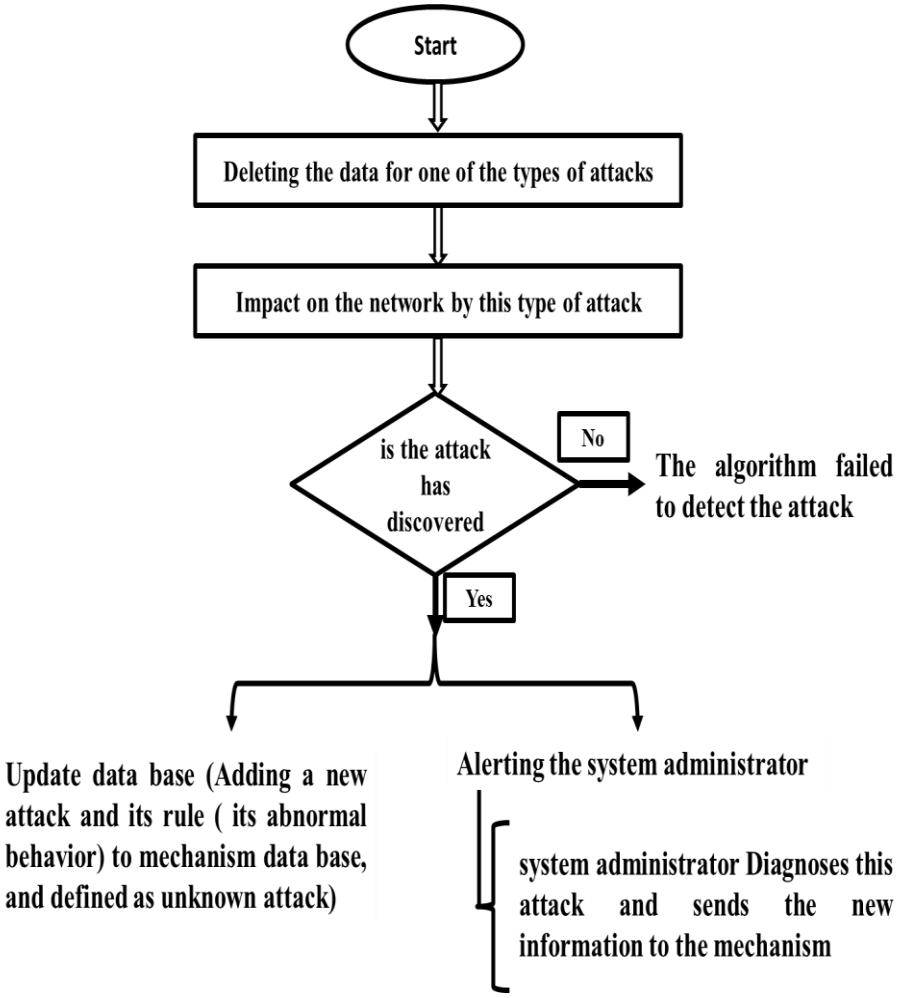


Figure.7: Diagram of mechanism work in learning phase

In this scenario we deleted the information of hello flood attack and the information of wormhole attack for 50 times for each attack.
Table7 shows the results for this scenario, the results show the detection rate, and as is clear in the table6, the detection rate for hello flood attack is 96%, and for wormhole attack is 92%.The average of detection rate is 94%.This indicates efficiency and effectiveness of mechanism.

Table 7. Detection Rate (DR) for wormhole and hello flood attacks

Type	Size	Number of Detection	DR%
Wormhole	50	48	96%
Hello Flood.	50	46	92%
	Average of detection rate		94%

IX. Conclusion

This paper presented a mechanism to protect WSN from external attacks. That mechanism can detection many types of unknown and known attacks. The result shows that the mechanism performs optimally.
The future research is to building test bed and taking the real results.

X. REFRENCES

[1] C. Karlof and D. Wagner: Secure Routing in Wireless Sensor networks: Attacks And Countermeasures, Ad Hoc Networks, vol. 1, pp. 293-315, 2003.
[2] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," ACM Trans. Sensor Networks, vol. 5, no. 1, Feb. 2011.
[3] Saurabh Singh Dr. Harsh Kumar Verma, "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering (IJCSE), 2011, 2393- 2399.
[4] Yi-an Huang , Wei Fan , Wenke Lee , Philip S. Yu: Cross-feature analysis for Detecting Ad-Hoc Routing Anomalies, Proceedings of the 23rd International Conference on Distributed Computing Systems, p.478, May 19-22, 2003.
[5] Zhihua Hu, Bochun Li, "Fundamental Performance Limits of Wireless Sensor Networks", 2004, pp. 81-101.
[6] Gaurav Sharma, Suman Bala, A K Verma and Tej Singh. Article: "Security in Wireless Sensor Networks using Frequency Hopping." International Journal of Computer Applications 12(6):15, December 2010, 1-5.
[7] Dorothy E. Denning, "An intrusion detection model. IEEE transactions on Software Engineering". IEEE, 1987. pp. 222- 232
[8] Youcai Zhou, Tinglei Huang, "A Statistic Anomaly Intrusion Detection Method For WSN, Microcomputer information", 2009.
[9] Libin Yang, Dejun Mu, Xiaoyan Cai, "An Anomaly Detection Scheme for Wireless Sensor Networks Based on Kernel Clustering", Journal of Sensors and Actuators• 2008.
[10] Wang Huaibin,YuanZhang. "Intrusion Detection for Wireless Sensor Networks Based on Multi-agent and Refined Clustering". Communications and Mobile Computing, 2009, pp. 450-454.
[11] Qi Zhu Rushun Song, Yongxian Yao, "SVM-based cooperation intrusion detection system for WSN", Application Research of Computers, 2010, pp. 1489-1492.
[12] Yang Liu,Yu Fengqi, "Immunity-based intrusion detection for wireless sensor networks", IEEE World Congress on Computational Intelligence, 2008, pp. 439 – 444.
[13] Sarjoun S.Doumit, Dharma P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", MILCoM :IEEE Military Communications Conference.2003, pp. 609-614.
[14] Vinay Soni1, Pratik Modi, and Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network", IJAIEM, 2013, pp. 29-32.
[15] V. Manjula and C. Chellappan, "TRUST BASED NODE REPLICATION ATTACK DETECTION PROTOCOL FOR WIRELESS SENSOR NETWORKS", Journal of Computer Science 2012, Pp. 1880-1888.
[16] Zorana Banković , David Fraga, José M. Moya and Juan Carlos Vallejo, "Detecting Unknown Attacks in Wireless Sensor Networks That Contain Mobile Nodes", sensors, 2012, Pp. 10834-10850.
[17] K. Fall and K. Varadhan, "The ns manual", User's manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009. Pp. 1-433.
[18] Aashima Singla, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks", IJARCSSE, 2013, pp. 529-534.