SELF-PROTECTION MECHANISM FOR WIRELESS SENSOR NETWORKS

Hosam Soleman[1] Dr. Ali Payandeh[2]

[1] Department of ICT Maleke-Ashtar university Islamic Republic of Iran
[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.

1. INTRODUCTION

The widespread use of wireless sensor networks, 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]. 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. And that the security requirements for wireless sensor networks have certain privacy was due to mind these requirements when designing a security mechanism.

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.

2. SECURITY IN WSN

Publishing wireless network in insecure environments, and using the wireless transmission, and the Limited sources, all of that making the security the important issue for the WSN. Therefore the security requirements (Authentication, Integrity, Confidentiality, Scalability, and Self-Organization) are very important for WSN [2].

DOI : 10.5121/ijnsa.2014.6307

A. Authentication

Authentication for WSN provides ensure to sender node and receiver.

B. Integrity

Data integrity is to ensure that information is same during transmission by using some security key for ensure

C. Confidentiality

The confidentiality means create security from unauthorized parties and attacker.

D. Scalability

Scalability is an important security requirement for designing an active and efficient routing protocol for WSNs.

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 [3].

E. Self-Organization

Due to the deployment of wireless networks in different environments and independent nature of the sensors, the sensors must be able to Self-Organization. [4].

3. Limitations of WSN

Wireless networks are characterized much of the specifications and Inherent limitations [5](storage, processing and transmission power and network connectivity and network lifetime... etc.) [6] That distinguish them from other networks and that must be considered when designing any security algorithm. These limitations are [7-8-9]:

1. Data transmission rate and lifetime of sensor network.
2. Random Topology.
3. Sensor Energy.
4. Ad-Hoc Deployment.
5. Fault Tolerance
6. Communication and environmental.
7. Expensive.

4. 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 [10]. 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[11], Cluster[12], Data Mining, Immunization Methods[15], Multi-agents[13], Neural Network, Support Vector Machine(SVM) [14],Hidden Markov Model [16].
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..

5. 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.

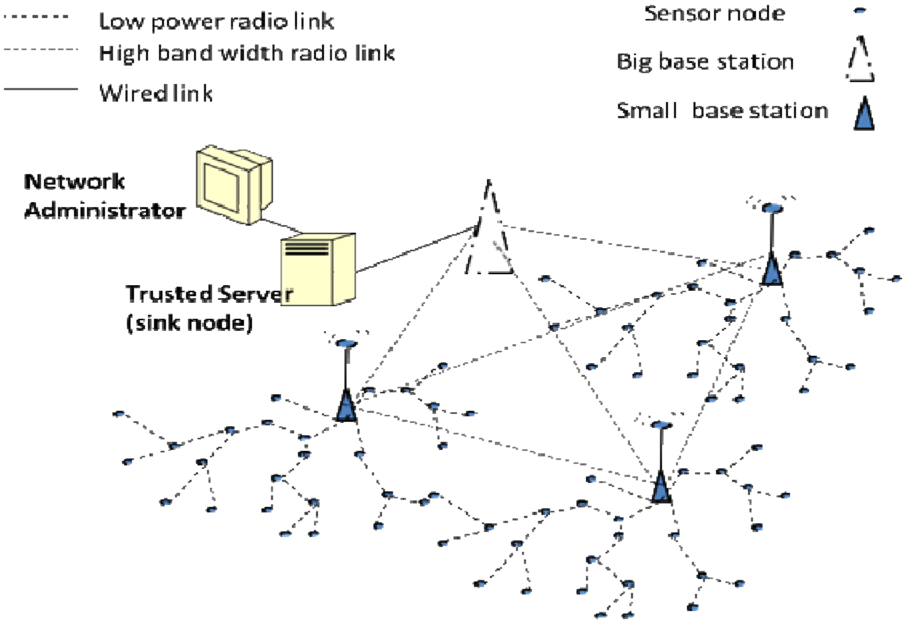


Fig1. Clustering of wireless sensor networks diagram

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.

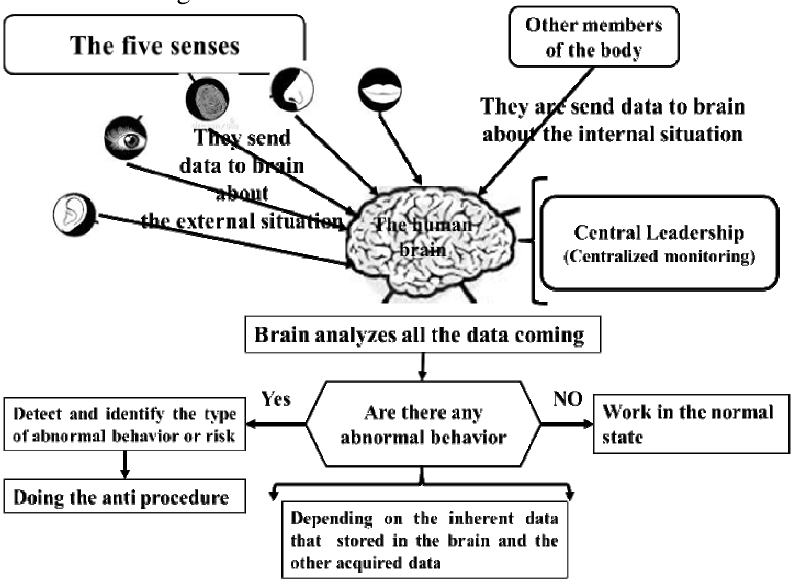

The five senses
Other members of the body
They send data to brain about the external situation
They are send data to brain about the internal situation
The human brain
Central Leadership (Centralized monitoring)
Brain analyzes all the data coming
Are there any abnormal behavior
Yes
NO
Detect and identify the type of abnormal behavior or risk
Doing the anti procedure
Work in the normal state
Depending on the inherent data that stored in the brain and the other acquired data

Fig2. Detecting the abnormal behavior by the brain

Figure 3 shows the work diagram.

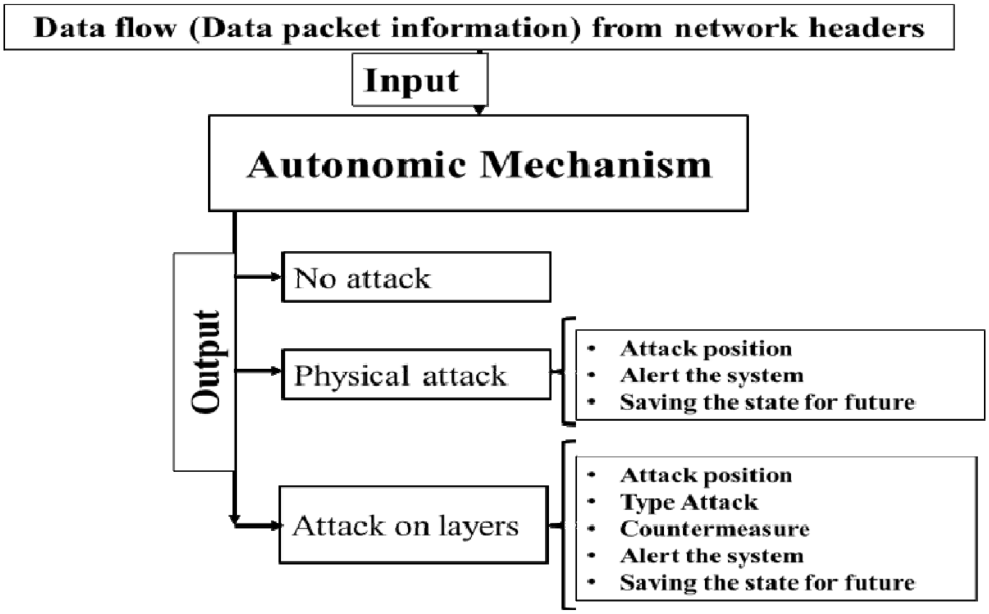


Fig3. Work diagram

Figure 4 shows the protection mechanism.

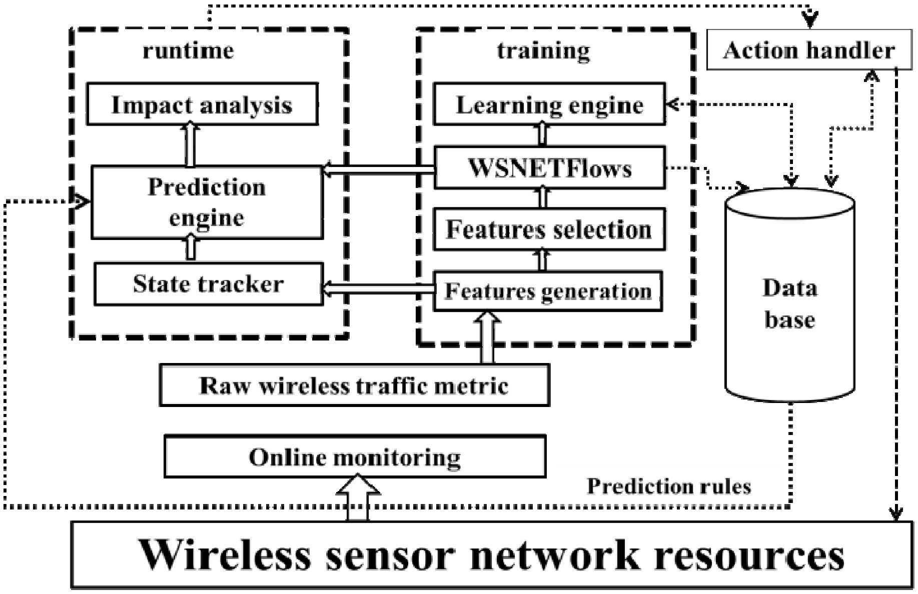


Fig4. Central protection mechanism

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).

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

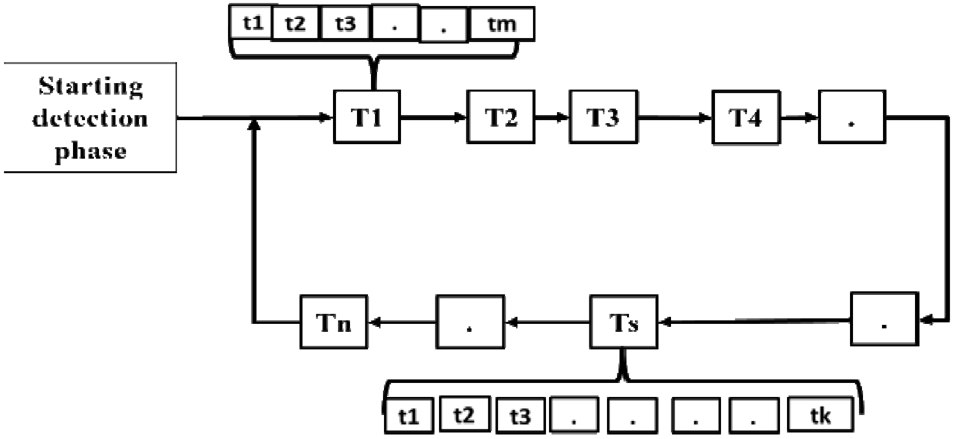
Network Nodes	*Packet Delivery Signal Strength*
Node0_ID	
Node1_ID	
Node2_ID	
.	
Noden_ID	

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.

When the self-protection mechanism completing testing all data flow form headers, the mechanism starting to test the packet flow and information the receiving from headers at the first point. As shown in the figure 5



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

Fig.5 Split test time

3. Attack Response

In this phase the self-protection mechanism does the following steps:

- 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.

6. Evaluation Self-Protection Mechanism:

In order to evaluate the mechanism has been used:

- **Detection rate:**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:

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

  - The 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.

- **The Impact of The Number of Attacks on Detection Rate.**
- **The Impact of The Number of Attacks on The Detection Time.**

7. Simulation Results

We used the Ns-2 simulator to evaluation self-protection mechanism [17]. The simulation parameters are:

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, number of CH (cluster head) nodes: 8 heads, number of base station node: one base station, an number of sensor nodes: 80 sensor.

We run this simulation for many times with affective with the effect of several types of attacks (Unfairness Attack, Wormhole Attack, Hello Flood Attack, Sybil Attack, Sinkhole attack, Exhaustion attacks, Collision Attack, and Selective Forwarding Attack [18]. We have successfully detected the attacks. The simulation results for detection rate shown in figure 6.

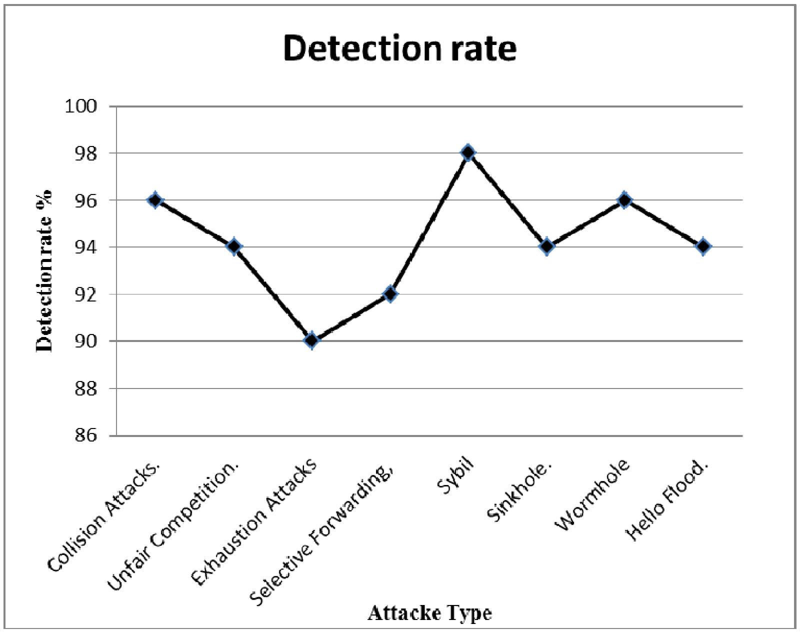


Figure6. Detection rate

The result shows that the mechanism performs optimally, And Average detection rate of more than 90% for all types of attacks.

Figures 7, 8, and 9, show the impact of the number of attacks on detection rate in case hello flood, sinkhole, and wormhole attacks.

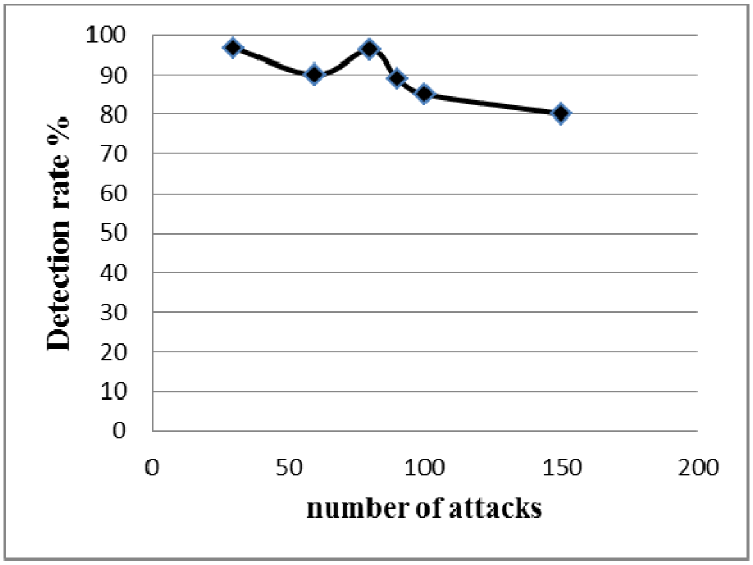


Figure 7 Effect of number of hello flood attack on detection rate

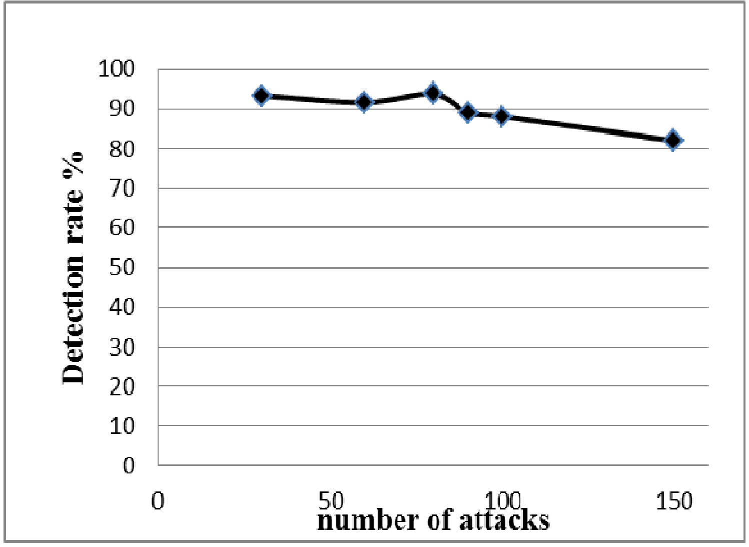


Figure 8 Effect of number of wormhole attack on detection rate

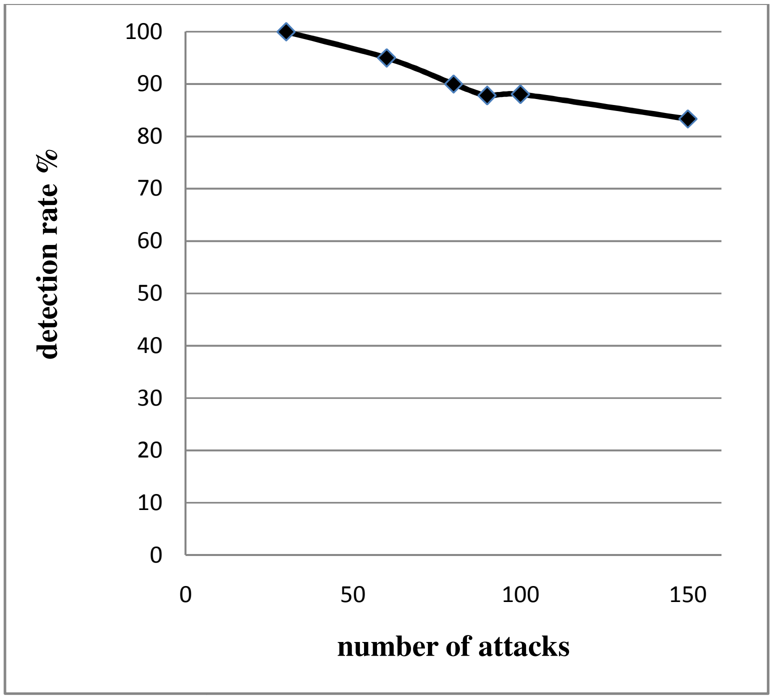


Figure 9 Effect of number of sinkhole attack on detection rate

As is shown in the previous figures (Figures 7, 8, and 9) increasing the number of attacks effect on the detection rate, but as noted, detection rate remained above 90% and this shows the efficiency of the mechanism.

Figures 10, 11, and 12, show the impact of the number of attacks on the detection time. in case hello flood, sinkhole, and wormhole attacks.

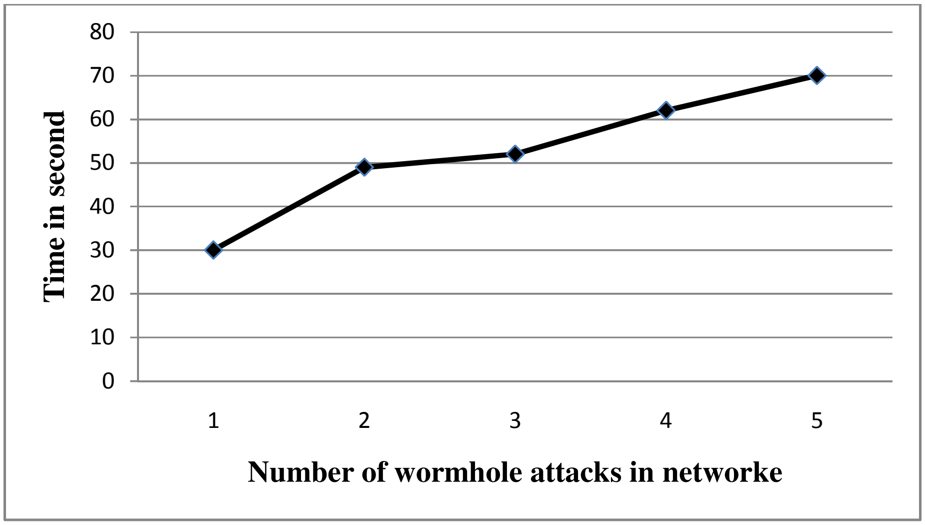


Figure10. Time token to detect wormhole attack

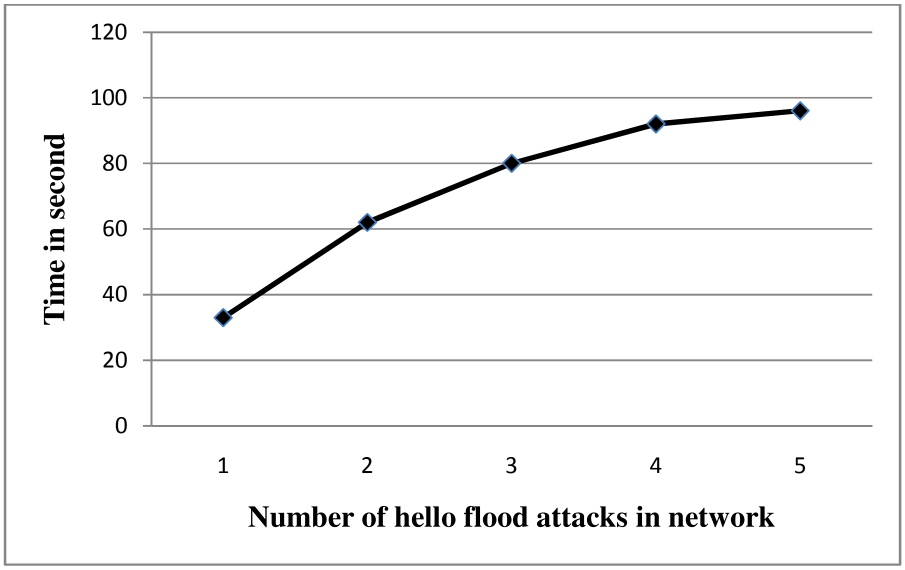


Figure11. Time token to detect wormhole attack

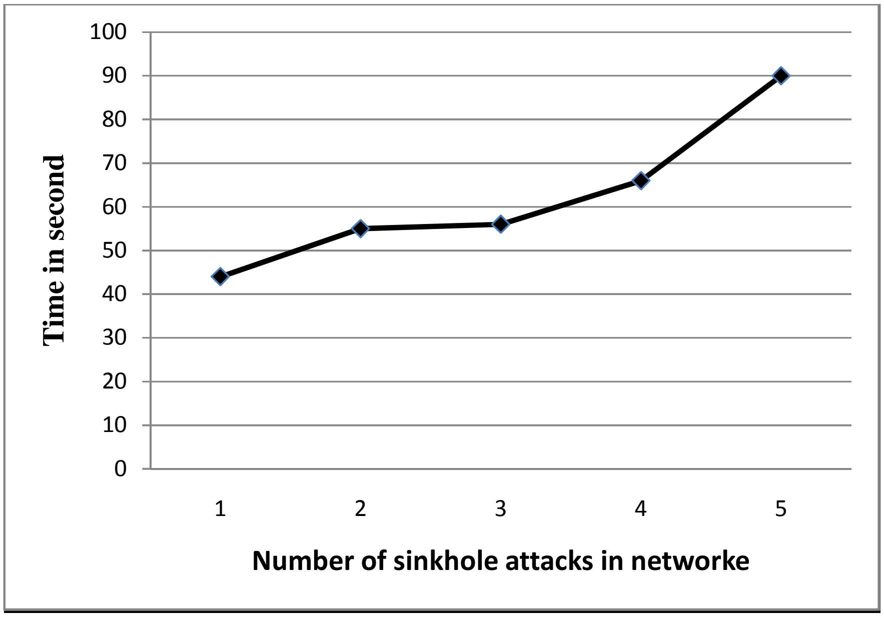


Figure12. Time token to detect sinkhole attack

As is shown in the previous figures (Figures 5.11, 5.12, and 5.13) increasing the number of attacks effect on the detection time, but as noted, detection time remained less than 90 second and this shows the efficiency of the mechanism

8. 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.

9. 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] Saurabh Singh Dr. Harsh Kumar Verma, “Security For Wireless Sensor Network”,International Journal on Computer Science and Engineering (IJCSE).

[3] L. Alazzawi and A. Elkateeb, “Performance Evaluation of the WSN Routing Protocols Scalability”, Journal of Computer Systems, Networks, and Communications, 2008, Pp1-10.

[4] A nserGhazzaal Ali Alquraishee and JayaprakashKar, “A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks”, Contemporary Engineering Sciences, 2014, 135 – 147.

[5] Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, “MoteSec-Aware: A Practical Secure Mechanism forWireless Sensor Networks”, IEEE, 2013, 2817-2829

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, “An effective key management scheme for heterogeneous sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 24–34, 2007.

[7] 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.

[8] ZhihuaHu,BochunLi,"Fundamental Performance Limits of Wireless Sensor Networks".

[9] Gaurav Sharma, SumanBala, 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.

[10] Dorothy E. Denning,An intrusion detection model.IEEEransactions on Software Engineering.1987.

[11] Youcai Zhou, Tinglei Huang, A Statistic Anomaly Intrusion Detection Method For WSN, Microcomputer information ,2009(in chinese).

[12] Libin Yang, Dejun Mu, XiaoyanCai, An Anomaly Detection Scheme for Wireless Sensor Networks Based on Kernel Clustering•, Chinese Journal of Sensors and Actuators•C2008.8(in chinese) .

[13] Wang Huaibin,YuanZhang.Intrusion Detection for Wireless Sensor Networks Based on Multi-agent and Refined Clustering[C].Communications and Mobile Computing•C2009.

[14] Qi Zhu Rushun Song, YongxianYao,SVM-based cooperation intrusion detection system for WSN,Application Research of Computers,2010.4(in chinese).

[15] Yang Liu,YuFengqi,Immunity-based intrusion detection for wireless sensor networks,IEEE World Congress on Computational Intelligence•C2008.

[16] SarjounS.Doumit, Dharma P. Agrawal, Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks, MILCoM :IEEE Military Communications Conference.2003.

[17] K. Fall and K. Varadhan, "The ns manual", User's manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009.

[18] Mohammad Sadeghi, FarshadKhosravi, KayvanAtefi, Mehdi Barati, "Security Analysis of Routing Protocols in Wireless Sensor Networks", IJCSI, 2012, 456-472.