Stackelberg Game between Multi-Leader and Multi-Follower for Detecting Black Hole and Warm Hole Attacks In WSN

S.Suganthi,
Research Scholar, Mother Teresa Women's University, Kodaikanal

Dr.D.Usha,
Assistant Professor, Mother Teresa Women's University, Kodaikanal

Abstract
Objective:

- To detect black hole and warm hole attacks in wireless sensor networks.
- To give a solution for energy depletion and security breach in wireless sensor networks.
- To address the security problem using strategic decision support system.

Methods: The proposed stackelberg game is used to make the spirited relations between multi leaders and multi followers. In this game, all cluster heads are acts as leaders, whereas agent nodes are acts as followers. The game is initially modeled as Quadratic Programming and also use backtracking search optimization algorithm for getting threshold value to determine the optimal strategies of both defender and attacker.
Findings: To find optimal payoffs of multi leaders and multi followers are based on their utility functions. The attacks are easily detected based on some defined rules and optimum results of the game. Finally, the simulations are executed in matlab and the impacts of detection of black hole and warm hole attacks are also presented in this paper.
Novelty: The novelty of this study is to considering the stackelberg game with backtracking search optimization algorithm (BSOA). BSOA is based on iterative process which tries to minimize the objective function. Thus we obtain the better optimization results than the earlier approaches.
Keywords:
Stackelberg Game, Black hole attack, warm hole attack, backtracking search optimization.

1. Introduction

Game theory is one of the interactive decision-making methodology which follows the techniques in a mathematical way. Generally, a formal game should consist of three elements such as the players of the game, the techniques are available for each player, and the optimal payoffs of each player. In a proposed stackelberg game contains multi leaders and multi followers[1]. The followers take the decisions based on their leader's decision. In a proposed game the cluster head acts as multi leaders which can optimizes the major upper level problem and all other agents nodes acts a followers who joined with leaders which can handle the lower-level problems. Generally, the follower take a decision after observing the leaders decision and the leader expect the response from the follower and selects their own optimal strategy for taking a decision. At the same time, all followers select their own optimal responses by competing with each other by the leaders choice. Many researchers doing their research in [2] Stackelberg game and applied wide applications in various areas. In a proposed game in this paper, several cluster heads can act the position as leaders and the remaining players can act as the position as followers, it becomes a multi-leader-follower game. Multi-leader-follower game[3] take place from some oligopoly markets[4]. For example, the large care companies called as the leaders have produce new-fashioned cars they make the decision to produce the cars and quantities [5]. After observing the decisions of the large car companies (leaders), all other smaller companies (followers) choose their optimal strategies to produce the quantities and qualities of the cars followed from the leaders[6]. Generally the attacks characteristics of warm hole is two malicious or attacker node combined together to make a tunnel[7]. The attacker node automatically receives the packet and sends it to other destination node through the tunnel without the knowledge of the network[8]. Due to this attack the attacker node may drops all the packets or make the changes of original node behavior. In a black hole attack, the attacker or malicious node falsely advertises the shortest path to all neighboring nodes. It will automatically generate a black hole region by sending the fake route to all other nodes.

The rest of the paper is organized as follows. Section 2 presents a detailed study of related work, section 3 describes the proposed network model and section 4 formulates the game between players. Section 5 gives a brief overview of strategic space Section 6 discusses the experimental results obtained using MATLAB and section

Manuscript received August 5, 2023
Manuscript revised August 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.8.19

7 concludes the paper by giving some ideas for future work in section

2. Network Model

Many papers describe the taxonomies of different layers attacks. Most of those papers show attacks classified by protocol stack layers(9). Some of papers show attacks classified on passive and active presented TPP Game algorithm that aims at modeling, analyzing the cooperation and trustable behavior between the nodes. In presented the Stackelberg game framework was employed to model and analyze the transmitting-jamming problem, and the anti-jamming power control game was investigated in wireless networks. In the cooperative transmission game was studied, and the equilibrium solution was obtained. In the authors formulated an attacker-defender Stackelberg game(10) between a jammer and a target node, and the timing channel was exploited. In a secure offloading game was formulated, and the Stackelberg equilibrium was derived. In we investigated the anti-jamming channel selection problem in an adversarial environment, and proposed a hierarchical learning approach to obtain the desirable solutions. Note that a survey on the jamming and anti-jamming techniques in wireless networks can be found in. Therefore, the rapid detection of the worm outbreak propagation in the IoT with limited resources by IDS has become an urgent problem to be solved(11). Herein, such IoT devices with embedded IDS are collectively referred to as “sensors”. The "scheduling strategy" mentioned in the following chapters of this paper is mainly aimed at methods of “sensor” combination opening(12).

3. Network Model

Network Topology

The network topology of the proposed system for analyzing Black hole and warm hole attack is given in figure 1.

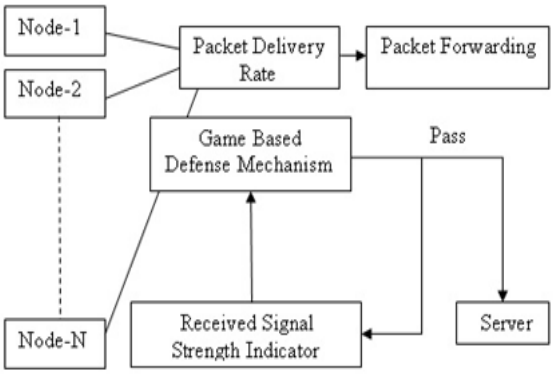


Figure 1 - Network Topology

Received Signal Strength Indicator (RSSI) is the measured power of a received radio signal [9]. The attacks are detected based on Packet delivery Rate (PDR) and Packet Forwarding Rate (PFR). Threshold RSSI value for black hole attack is $T_{rssi\_bh} = -40$. Threshold RSSI value for warm hole attack is $T_{rssi\_wh} = -55$. Threshold Packet delivery rate in black hole attack is $T_{pdr\_bh} = 90$. Threshold value of packet delivery rate in warm hole attack is $T_{pdr\_wh} = 80$.

The cluster head has selected using particle swarm optimization refer as Figure 2. During the transmission of data from cluster head to all other agent nodes refer in figure 3, some attacker node may indicate highest Received Signal strength value and packet delivery rate.

All the received values are recorded. In this situation some normal nodes may choose wrong path. If the newly generated RSSI value may exceed the threshold RSSI value then it will be assumed as some nodes may affect by a black hole attack.

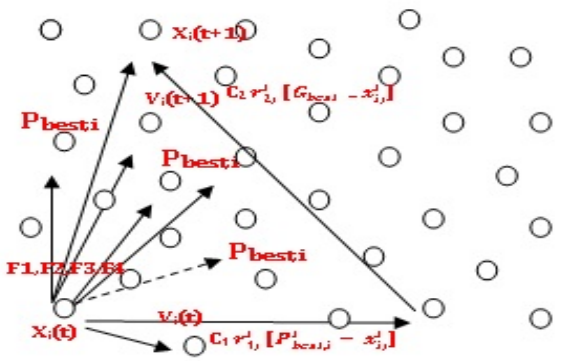


Figure 2 - Cluster Head Selection

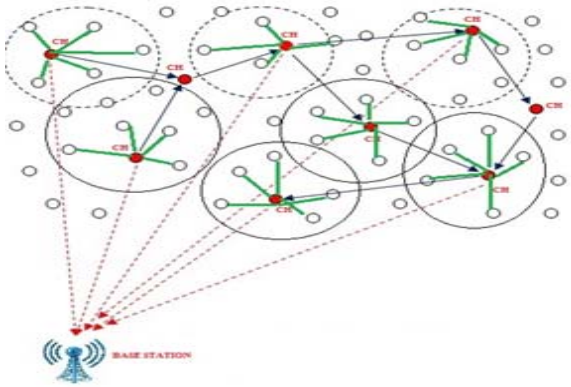


Figure 3 - Node Transmission

During the path finding process, some attacker node can automatically create a tunnel with some other attacker node. So the packet delivery process may automatically deviate the valid route to wrong route. In this scenario the Received signal strength value and packet delivery rate can be monitored. If the monitored value is greater than threshold received signal strength value and packet delivery rate then it is assumed as some nodes may affect by a warm hole attack is illusted in figure 4.

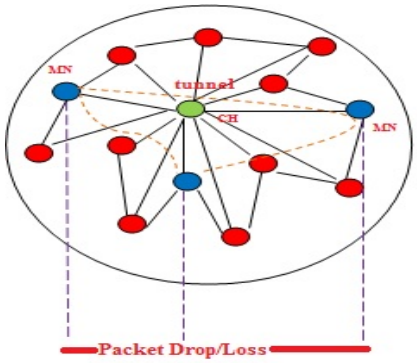


Figure 4 – Packet Drop / Loss

The proposed algorithm can compute the threshold Received Signal Strength Indicator value and Threshold Packet delivery rate value. The threshold value is based on bandwidth, data flow rate, link strength, outcome of the defender. The threshold value T automatically passes to the indicators of the game. The proposed game which decides whether to allow the packets or redirect or drop a data flow based on the Threshold value T.

4. Game Formulation

Game theory is the formal, mathematical methodology for interaction between players like people, agents or robots which has been applied in diverse areas such as business, economics, and management to solve problems. In this section we have identified the attacked nodes through some gaming strategy. Competition among the players is one of the significant topics.

We use stackelberg game model which is applied to find the best non malicious nodes in a sensor environment is depicted in figure 5.

In a Stackelberg model, leader chooses a strategy first and then follower observes this decision and makes his own strategy choice. Intuitively, the first player chooses the best possible point based on the second player's best response function. Generally the game includes the following three comprise:

Player set: Players set contains Leaders and Followers
Leaders denoted as N
Followers denoted as M

Strategy set: A - Denotes the set of actions, i-denotes the strategy. The set of actions of a game is denotes as $A = A_1 \times A_2 \times \ldots \times A_n$. a-denotes the player which is defined as $a_i \in (a_i, a_{-})$ a_i denotes the player a with i strategy while a_{-i} denotes other players' strategies.

Utility functions: The utility function or outcome of player i denoted by u_i (a_i,a_{-i}). The payoff function is measured by outcome of i^{th} player strategy and other players' strategies. In a game theory players are considered rational decision makers they choose the best strategy to maximize their benefit function.

5. Players and the Strategic Space

We establish a Stackelberg game between the defender and attacker. Practically the cluster head plays the role of the game leader and makes the first move by choosing its detection strategy whereas all other agent nodes are acts as the followers that observe the leader's strategy and choose their best responses to it in terms of attack detection strategies is illustrated in Figure 5.

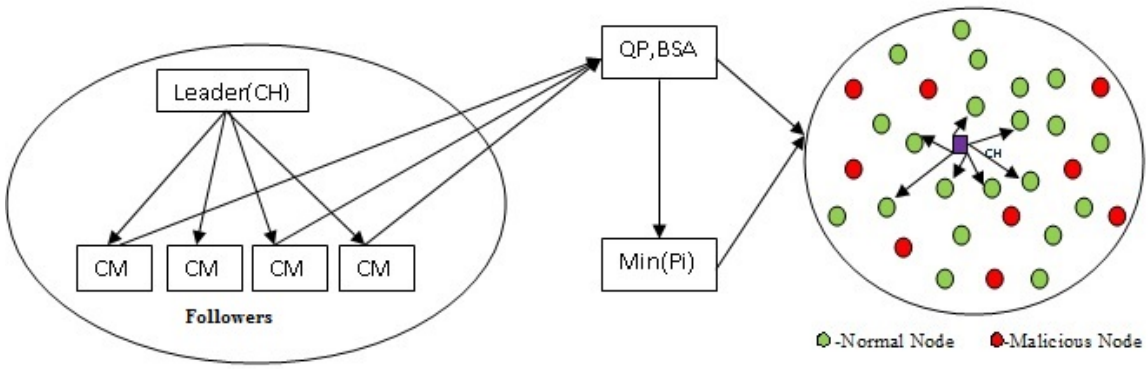


Figure 5 – Stackelberg Game

The game is modeled initially as Quadratic Programming. The backtracking search optimization for getting threshold value to determine the optimal strategies of both defender and attacker.

Quadratic Programming:
Quadratic programming is a special class of non linear optimization problem. We assume quadratic Objectives:
$Q_L(P_L,P_F)$; L- Leader, F-Follower, P-Players , $Q_F(P_L,P_F)$ with the structure

$$Min\, f(x) = \frac{1}{2} X^T Q X + C^T X$$

Subject to AX= b, x≥0
Is given by the linear system

$$\begin{bmatrix} Q & E^T \\ E & 0 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} -C \\ d \end{bmatrix}$$

Quadratic Programming for Leader and follower:

$$X = \begin{bmatrix} P_L \\ P_F \end{bmatrix}$$

$$Q_L = \frac{1}{2} \begin{bmatrix} P_L \\ P_F \end{bmatrix}^T \begin{bmatrix} C_L^{LL} & C_L^{LF} \\ C_L^{LF} & C_L^{FF} \end{bmatrix} \begin{bmatrix} P_L \\ P_F \end{bmatrix} + \begin{bmatrix} C_{LL} \\ C_{LF} \end{bmatrix}^T \begin{bmatrix} P_L \\ P_F \end{bmatrix}$$

$$Q_F = \frac{1}{2} \begin{bmatrix} P_L \\ P_F \end{bmatrix}^T \begin{bmatrix} 0 & C_L^{LF} \\ C_L^{LF} & C_L^{FF} \end{bmatrix} \begin{bmatrix} P_L \\ P_F \end{bmatrix} + [C_{FF}]^T [P_F]$$

$Q_L, Q_F \geq 0$

All feasible regions must be a convex set that means all linear constraints Q_L, Q_F must be in convex set. To minimize the objective function, we have to reduce the radius of the circle. To find more than one variables we use khuntucker condition.

$$Min\, f(x) = \frac{1}{2} X^T Q X + C^T X$$

Subject to AX≤ b , AX-b≤0
X≥0, -X≤0

Khuntucker Condition

$$\nabla f(x) + \sum_{i=1}^{m} \lambda_i \nabla g_i(x) = 0$$

$$\lambda_i \nabla g_i(x) = 0 \;\forall\; i$$

$$g_i(x) \leq 0,\ \lambda_i \geq 0$$

$$\nabla f(x) = \left(\frac{\partial f}{\partial x_1} \frac{\partial f}{\partial x_2} \frac{\partial f}{\partial x_3} \ldots \ldots \frac{\partial f}{\partial x_n} \right)$$

Let us define two utility matrices for the leader and the follower

$U_L^{i,j} = R_{i,j}$ and $U_F^{i,j} = C_{i,j}$

In a multi leader follower game, the algorithm for Leader's Choice is as follows:

Algorithm 1: Leader's Choice
Input: Leader variables
Output: Objective function
N- Leader(L)
L=1…N
Decision Variable $x^L \in \mathbb{R}^{nL}$
Vector tuple $x := (x^1 \ldots . x^N) \in \mathbb{R}^n$
$n := \sum_{L=1}^{N} n_L$
$(x^L, x^{-L}) \in \mathbb{R}^{n_L + n_{-L}}$, $n_{-L} := n - n_L$
Objective function or Utility function
$\Theta_L : \mathbb{R}^{n+m} \rightarrow \mathbb{R}$ is dependent on x^L to x^{-L}, $\forall$ y
Leader Strategy :
x^L (x^{-L}) $\in \mathbb{R}^{nL}$ is dependent on x^L to x^{-L} and independent on followers y
Leader solve the following optimization problem
Min Q_L (x^L , x^{-L}, y)
Subject to $x^L \in X^L$
f(x,y):= ($\nabla_{x'}$, ΘL)

Algorithm 2: Follower's Choice
Input: Follower variables
Output: Objective function of follower
M-Follower(F)
F=1…M
Response Variable $y^F \in \mathbb{R}^{mF}$

Manuscript received August 5, 2023
Manuscript revised August 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.8.19

Vector tuple y:= $(y^1 \ldots . y^m) \varepsilon \mathbb{R}^m$
n:= $\sum_{F=1}^{M} n_F$
$(x^F, x^{-F}) \varepsilon \mathbb{R}^{m_F + m_{-F}}$, $m_{-F} := m - m_F$
Objective function or Utility function
$\Theta_F : \mathbb{R}^{n+m} \rightarrow \mathbb{R}$ is dependent on y^F to y^{-F} , $\forall$ x
Follower Strategy :
$Y^F (y^{-F}, x) \mathbb{R}^{mF}$ is dependent on leaders x
Follower solve the following optimization problem
Min $Q_F (x, y^F, y^{-F})$
Subject to $y^F \varepsilon Y^F$
$F(x,y) := (\nabla_{y'}, \Theta F)$

Backtracking Search Optimization

After applying quadratic programming we can get the optimized nodes. Generally backtracking search is applied to have multiple solutions and need all those solution. Backtracking algorithm which is mainly used to execute a multiple sequence of decisions, which is performed recursively until satisfying certain constraints.
G_{min}= Global Minimizer Game matrix
$G_{\min_{zer}}$= Minimum of Minimum Game matrix
N= Number of agent nodes
D= population size
$P_{i,j}$= Player of i,j strategy
Pre $_{i,j}$ = All other players i,j strategy
fit_{pi} = Fitness function player with strategy i

Algorithm 3:

Input: $O_{func}, N, D, max_{cycle}, mix_{rate}, low , up, epoches$
Output:$G_{min}, G_{\min_{zer}}$
Step1: Initialization
1. $P_{i,j} \sim U(low_j - up_j)$ *// i=1..N , j=1..D,U- is the uniform distribution*

Step 2: Selection –IBSA has the option of redefining old population, it is used to randomly change the order of the individuals in old population
2. $G_{min} = inf$,D=30,N= $Agent_{node}$;
3. $P_{i,j} = \lim_{i \to 1 \text{ to } N} \lim_{j \to 1 \text{ to } D} (up_j - low_j) + low_j$
4. $Pre_{i,j} = \lim_{i \to 1 \text{ to } N} \lim_{j \to 1 \text{ to } D} (up_j - low_j) + low_j$
5. $fit_{Pi} = \lim_{i \to 1 \text{ to N}} O_{func}(P_i)$
6. $For \ y = 1 \ to \ max_{cycle}$
   $If (a < b) \ then \ Pre = P$
   $Pre = permuting(Pre)$ *// permuting function is a random shuffling function*

$Step\ 3: Mutation$
The mutation process generates the initial form of the trial population called M_{mut}
$M_{mut} = P + F\ (Pre - P)$ *// where F controls the amplitude of the search direction matrix*
$(oldp - p)$ *, the historical population is used in the calculation of the search-direction matrix.*
7. $M_{mut} = P + 3\ (Pre - P)$ *// 3 is random number ~ N(0,1)*

Step 4: Crossover
BSA's crossover process generates the final form of the trial population T. The initial value of the trial population is Mutant, as set in the mutation process. Trial individuals with better fitness values for the optimization problem are used to evolve the target population individuals. BSA's crossover process has two steps.
The first step calculates a binary integer-valued matrix (map) of size N. D that indicates the individuals of T to be manipulated by using the relevant individuals of P. If map n, m = 1, where n ϵ {1,2,3…,N} and m ϵ {1,2,3…,D}, T is updated with T n, m := P n ,m In Algorithm-2 (on line 3) indicates the ceiling function, defined as rand ~ U (0, 1). BSA's crossover strategy is quite different from the crossover strategies used in EA's and its variants. The mix rate parameter (mixrate) in BSA's crossover process controls the number of elements of individuals that will mutate in a trial by using ceil (mixrate. rand. D).
The function of the mix rate is quite different from the crossover rate used in EA's. Two predefined strategies are randomly used to define BSA's map. The first strategy uses mixrate. The second strategy allows only one randomly chosen individual to mutate in each trial. BSA's crossover process is more complex than the process used in EA's. Some individuals of the trial population obtained at the end of BSA's crossover process can overflow the allowed search space limits as a result of BSA's mutation strategy. The individuals beyond the search-space limits are regenerated using Algorithm-3.
8. $Cr_{1:N,1:D} = 1$
9. $If (c < d) \ then$
   For k=1 from N
   $Cr_{i,1:[mix_{rate} * rand(D)]] = 0$
   $End\ for$
   Else
   $For\ k = 1\ from\ N$
   $Cr_{k:rand(D)]] = 0$
   $End\ for$
   $T = M_{mut}$
   //Boundary control mechanism
   $T_{i,j} =$
   $\lim_{i \to 1 \text{ to } N} \lim_{j \to 1 \text{ to } D} \begin{cases} rand(up_j - low_j) + low_j & if\ (T_{i,j} < low_j)\ OR\ (T_{i,} \\ T_{i,j} & else \end{cases}$
   $End\ if$

Step 5: Selection – II
In BSA's Selection-II stage, the Ti's that have better fitness values than the corresponding Pi's are used to update the Pi's based on a greedy selection. If the best individual of P (Pbest) has a better fitness value than the global minimum

value obtained so far by BSA, the global minimizer is updated to be Pbest , and the global minimum value is updated to be the fitness value of Pbest. The structure of BSA is quite simple; thus it is easily adapted to different numerical optimization problems.

10. $fit_T = O_{func}(T)$
11. $fit_{Pq} = \lim_{q \to 1 \text{ to } N} \begin{cases} fit_{T_q} & if (fit_{T_q} < fit_{Pq}) \\ 0 & else \end{cases}$
12. $fit_{best} = \min(fit_P)$
13. If $fit_{best} < G_{min}$ *then*
    $G_{min} = fit_{best}$ *// the global minimum value is updated to be fitness value of population*
    $G_{\underset{zer}{\min}} = P_{best}$
    End if
14. *End for*

//detection of normal as well as malicious node

15. $label_{label} = \max(Best_{pos)} > mean(G_{\underset{zer}{\min}})$

$$Nor_{node} = \begin{cases} 1 & if \left(\max(Best_{pos)} > mean\left(G_{\underset{zer}{\min}}\right) \right) \\ 0 & otherwise \end{cases}$$

The follower employs the same strategy to find best nodes or any strategy with the same payoff.

Attack Model:

Blackhole and Warmhole Attacks:

In black hole attack, a malicious node advertises itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. The malicious node received the reply message by the requesting node before the reception of reply from actual node. Hence, a malicious and forged route is created. Because of the malicious node may indicate highest Received Signal Strength value(RSSI) and packet delivery rate(PDR).

If the newly generated RSSI value may exceed the threshold RSSI value then it will be assumed as some nodes may affect by a black hole attack. When this route is establish, it may happens whether to drop all the packets or forward it to the unknown address. The general scenario of blackhole and warmhole attacks is showed in Figure 6.

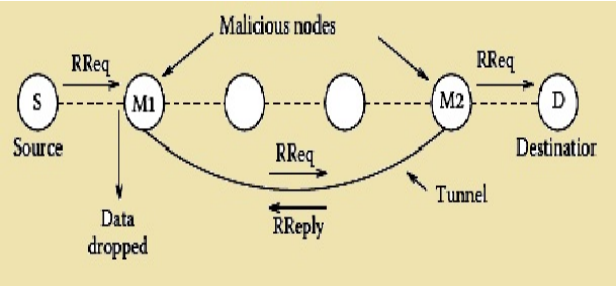


Figure 6 – Blackhole & Warmhole Attack

A wormhole attack is composed of two attackers through a wormhole tunnel. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel between them. A wormhole tunnel can be established by means of a wired link or a high quality wireless out of band links, or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors and forwards them to the other colluding attacker through the wormhole tunnel. This latter node receives these tunneled packets and replays them into the network in its vicinity. In a wormhole attack using a wired link or a high quality wireless out-of-band link, attackers are directly linked to each other, so that they can communicate quickly. On the other hand, a wormhole using packet encapsulation is relatively much slower. But it can be launched easily since it does not need any special hardware or any special routing protocol. In this scenario the Received signal strength value and packet delivery rate can be monitored. If the monitored value is greater than threshold received signal strength value and packet delivery rate then it is assumed as some nodes may affect by a warm hole attack.

Algorithm 4: Detection of various attacks

Input: $PDR\_node\_Id,\ RSSI\_node\_Id, DPR\_node\_Id$
Output: Malicious and normal node Attack ID

PDR- Packet Delivery Rate
RSSI-Received Signal Strength Indicator
DPR=Duplicate Packet Rate
For i=1:to size of N_x

$if\ (PDR\_node\_Id(i) > T_{pdr_{bh}} \&\& RSSI\_node\_Id\ (i) > T_{rssi\_bh}\ )$
$BH = i$
$elseIf\ (RSSI\_node\_Id\ (i) > T_{rssi\_wh} \&\& PDR\_node\_Id(i) > T_{pdr\_wh}\ )$
$WH = i$
else
$Nor\_node = i$
End if
End for

After applying all the above algorithms the optimum results can be obtained.

6. Simulation Results

The proposed algorithm can be implemented in matlab code and the convergence is calculated. The performance evaluation will be computed based on some parametric measures. The X-axis is denotes as number of nodes are taken. The Y-axis is denoted as Number of rounds the algorithm is going to be implemented. Numerical values used for evaluation as shown in Table 1,2,3,4,5,6 and the evaluation measures are depicted as Accuracy in figure 7, sensitivity shows figure 8, Figure 9 as Detection Rate, Figure 10 shows that F-Score, Figure 11 shows that False positive rate, Figure 12 shows that false negative rate of the proposed system.

Table 1 : ACCURACY

	20	40	60	80	100
overall	94.52518	97.15385	98.89155	98.74127	98.9011
BH	84.80255	89.28571	92.89041	95.38462	97.77419
WH	80.31325	87.2069	95.59459	96.93939	97.74468

Table 2: Sensitivity:

	20	40	60	80	100
over all	93.43697	95.59459	96.56098	97.2973	98.53922
BH	82.29197	85.36585	93.52326	94.30769	95.33962
WH	78.34247	83.39535	91.90909	93.58	924.5926

Table 3: Detection Rate:

	20	40	60	80	100
over all	98.8	98.9	99.8	100	100
BH	97.8	98.6	98.9	100	100
WH	97.7	98.4	99.5	100	100

Table 4: F-Score

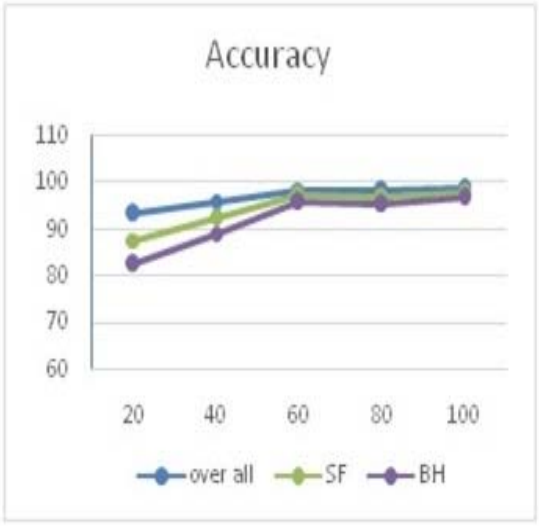
	20	40	60	80	100
over all	91.59034	93.70817	96.61836	96.35974	97.08738
BH	79.65243	84.64329	92.1659	91.46341	93.45794
WH	74.77906	80.73818	90.09009	89.19722	91.74312

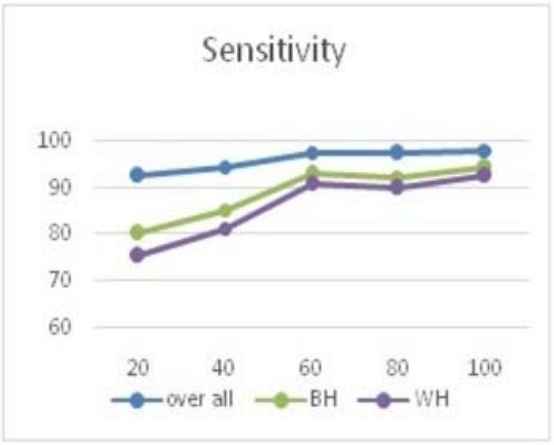
Table 5: False Positive

	20	40	60	80	100
over all	0.006	0.003	0.082	0.064	0.052
BH	0.005	0.001	0.073	0.014	0.002
WH	0.004	0.095	0.061	0.02	0.085

Table 6: False Negative

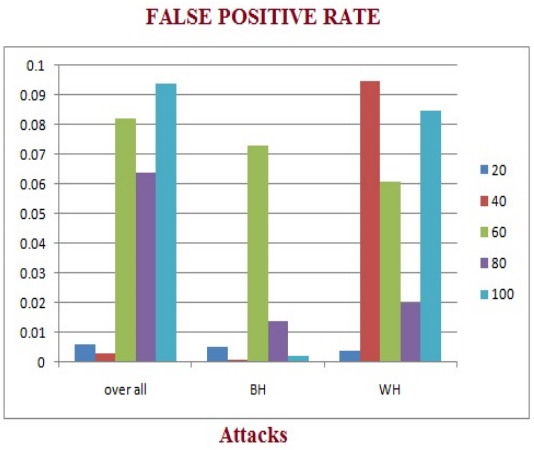
	20	40	60	80	100
over all	0.072	0.082	0.095	0.074	0.063
BH	0.063	0.061	0.093	0.002	0.066
WH	0.068	0.04	0.072	0.085	0.092

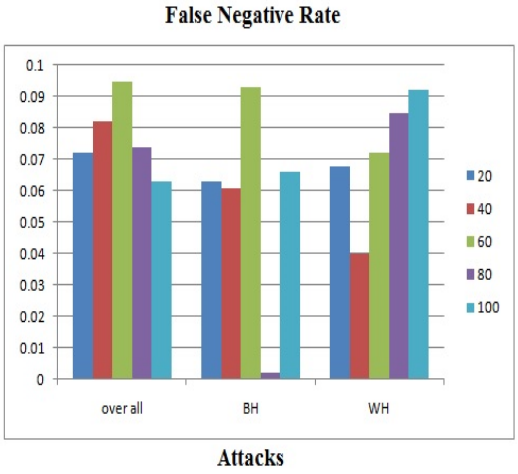

Accuracy
110
100
90
80
70
60
20
40
60
80
100
over all
SF
BH


Sensitivity
100
90
80
70
60
20
40
60
80
100
over all
BH
WH


Detection Rate
101
100
99
98
97
96
20
40
60
80
100
over all
BH
WH


F - Score
100
90
80
70
60
20
40
60
80
100
over all
BH
WH





7. Conclusion

Wireless sensor networks are seriously vulnerable to attacks, and their ability of resistance against the attacks is one of the critical challenges in the development of these networks. Security is recognized as a world-wide challenge and game theory is an increasingly important paradigm for handling security breaches. Two main weaknesses of the traditional intrusion detection systems are as follows: 1) from a technical perspective, they are highly complicated and 2) they rely on the temporary methods based on trial and error. Smart solutions have shown that although they have their own specific complexities, they are faster in speed and much more optimal in performance. The results obtained in this paper, which is based on the game theory, confirmed that smart methods can have better performance compared to the other strategies in terms of accuracy, specificity, detection rate and false alarm rate.

References

[1] F. Yao, L. Jia, Y. Sun, Y. Xu, S. Feng, and Y. Zhu. A hierarchical learning approach to anti-jamming channel selection strategies, 2017; 1-13. DOI: https://doi.org/10.1007/s11276-017-1551-9.

[2] Er.Harpal, Dr.Gaurav Tejpal and Dr.Sonal Sharma. Machine Learning Based Watchdog Protocol For Wormhole Attack Detection In Wireless Sensor Networks. International Journal of Computer Science and Information Security (IJCSIS). 2017; 15(9). 54-63. https://sites.google.com/site/ijcsis/

[3] Tamilarasi, N., Santhi, S.G. Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network. Wireless Pers Commun. 2020; https://doi.org/10.1007/s11277-020-07365-4.

[4] Dr. B. Padminidevi, Mrs.C.Selvarathi. Implementation Of Network Security Using Wormhole Attack. International Journal of Advanced Science and Technology, 2017; *29*(7s). 1643 - 1650. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/11051.

[5] Ruirui Zhang1and Xin Xiao. Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division. Journal of Sensors. 2019. 1-20 Doi: 10.1155/2019/5451263.

[6] Zulfiqar Ali Zardari, Kamran Ali Memon, Reehan Ali Shah, SanaullahDehraj, Iftikhar Ahmed. A lightweight technique for detection and prevention of wormhole attack in MANET.2020; 1-6. DOI: 10.4108/eai.13-7-2018.165515.

[7] Lina Mallozzi , and Roberta Messalli. Multi-Leader Multi-Follower Model with Aggregative Uncertainty. 2017; 8(25). doi:10.3390/g8030025.

[8] Lili Chen,Zhen Wang,Fenghua Li, Yunchuan Guo and Kui Geng. A Stackelberg Security Game for Adversarial Outbreak Detection in the Internet of Things. 2020; *20*(804), doi:10.3390/s20030804

[9] Mehetre, D., Roslin, S., & Wagh, S. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. 2019; *Cluster Computing,* **22**, 1313–1328. https://doi.org/10.1007/s10586-017-1622-9.

[10] Pedro Manso et.al. SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks. Information 2019, 10, 106; doi:10.3390/info10030106.

[11] Muhammad Asim Khan, Mansoor Khan. A Review on Security Attacks and Solution in Wireless Sensor Networks. American Journal of American Journal of Computer Science and Information Technology. 2019; 7 (1: 31). 1-7. DOI: 10.21767/2349-3917.100031

[12] Zeljko Gavric1, and Dejan Simic. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingenieria e Investigation. 2018; 38(1). 130-138. DOI:10.15446/ing.investig.v38n165453.