Energy Consumption Patterns Paving Way To Isolate Black Hole Attack in WSN

Upekha Sharma, Sunita Gupta
Department ofComputer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan Jaipur-302017 (INDIA)
Email: upee_ish@yahoo.co.in, drsunitagupta2016@gmail.com

Received 27.07.2019 received in revised form 10.08.2019, accepted 06.10.2020

Abstract-Sensors embedded in wireless mesh nexus calls for widely acclaimed area of research, due to its framework and internal components that integrate and work in synchronization mainly for perception of information. Being the backbone potential to various fields and applications, like critical infrastructure, disaster recovery situations, object and inventory tracking, health and medical setup, wireless sensor network has caught the attention of intruders to extract the information or disrupt its transmission. Sensor nodes are geographically aligned in mesh architecture, doing the needful. This paper revolves around the well-known "Black Hole Attack" by probing its behavior in depth and also detecting it in view of various parameters. The put forth technique focuses on energy consumption model primarily and different energy parameter values are recorded under the Invasion-case and Non-invasion case. The simulation and experimental results hence forth prove the presence of malignant attacker.

Keywords –WSN, Blackhole, Packet, Energy consumption, Attack, Data, sensor nodes, Send, Receive, Forward, Drop, Security, malicious.

1. INTRODUCTION

Wireless divulgence involves the interchange of particulars among two or more stations over a fickle medium. The cellular divulgence technology makes use of radio waves to transport facts among the logically nodes. WSN is one of the application domains of wireless communication. WSN is a distributed computing architecture comprising resource available at contrived units that work in an impromptu fashion over multi-hop interaction [1].

Some of these important applications include environment analyzing, infrastructure governance, public shield, medical and fitness prudence, home and workplace welfare, and military indulgences [2].

Progression in leaps and bounds pertaining to semiconductor technology and development of more efficient broadband cellular mechanics have paved way to the deployment of more efficient WSNs in terms of cost, speed and space, thus bridging the gap between WSNs and the outside world. These wireless mesh nexus ambits are filled with many dispersed but sovereign bodies which join hands to check on real world scenarios.

Present day technological evolution in coherent circuit elevation, has built the feasibility for the lineup of tiny, reasonable, rock bottom competence, apportioned widget with the potential of running provincial processing and cellular circulation [3]. But when they accumulate and integrate the information from a massive count of other entities, they have the skillfulness to record a physical ambit at hand at length. To conquer the energy efficiency and preservation in WSN, the mentioned approach levies certain constraints like Q-coverage and P-connectivity on functioning of node to enhance the time span of WSN [4].

These spaces of functional zones are unlatched to be pounced upon. The zones incur shelling performed by malicious nodal units.

Malignant node cascades are considered to be silent murderers of WSN. These knobs are lodged explicitly by the invader into the secure surroundings so as to enforce malicious strikes. In the endeavor the virus node is pondered in order to perform blackhole attack.

Many disparate varieties of ambushes are in the records to have existed in a Sensor inclusive wireless network composing of burlesquing the numerous segments of an information box while it is on the go. Operation on the hamper involves tactful scheme that the devisee attains a refashioned version in place of true message that is generated by the starting station [5]. The denial of service attack has gained popularity by the fashion that a malicious node follows by sucking all data caskets by erroneously professing a fresh road to the terminus station. The bomber uptakes every hamper that are in their pursuit to the finish line.

The packet drizzle attack narrated as black hole unit invader is illustrated in the research that encircles a malignant body drinking away all the data packets depicting role of the black hole in the universe that sucks in everything that approaches to it. It plays on the gross cumulative culpabilities towards the path unearthing containers of the on demand protocol called AODV [6].

Indeed the blackhole strike in WSN moulds a tradeoff road inception in a network. An abnormal entity that relays a routing note having an astounding high power is able to deceive an enormous count of nodes. An identical scenario is viewed in blackhole attack acting as a malicious node persuades all nodes in its proximity to be just a single leap from terminus unit those are in real manifold leaps from the sink nodal bod. The persuaded entities in retaliation venture to dispatch their caskets straight away to the sink station unit, which fails to discern them [7].

The incompetency of resident security masks that yield them fruitless signals for devising coherent models in order to comply with the unerring exercising of Wireless sensor based Nexus, especially in an infected ambience or pertaining to internal invasions. The compromised node, which comprises the network, behaves as a statutory node. This problem aims the main research that remains open is “How can internal shelling be overcome to win a taut WSN”. Therefore, the predominant intent governing the paper moves to build a potent mechanism to shield WSNs from internal attacks.

2. RELATED WORK

To hike up the network capacity, WSNs follows multi-hop communication. The sensor nodes are not cushioned as they are cut price and are embedded in unbolted territory where these nodes lose themselves to be effortlessly compromised. The compromised node opens door for an attacker to access the sensitive information and can kick off malicious engagements.

Renowned researcher [8] proposed an algorithm that was run on AODV (Ad hoc on demand Distance Vector) Routing protocol. The proposed plan of action was able to surface both the Cooperative Black hole shelling accompanied by single Black hole bomb. The algorithm initializes with first step engaging in fingering of black hole bodies from the nexus and then accordingly their listings are threshed from within the routing list. The chief benefit of the plot was it could diagnose blackhole attack node in both the cases, when it is in active or in idle state.

A team came up with the notion and [9] have plotted a two-pleat strategy for the unearthing and quarantine of units we call burls that cater to drizzle of the data hampers. In the First shot, it strives on a look out for the secretive action gunned by nodes and also aims to pinpoint the viral activities in network. This can be effectuated by dispatching an ACK packet to the father node by all the intermediate nodes and thus provides the affirmation of triumphant reception of data packets. If the ACK packet send by intermediate nodes is not gained by originator node, who takes on to replay the packet for terminus passing a time interval. If the twin activity was visualized yet once more, the originator node then releases a hamper that announces the presence of viral pursuits in the mesh network. The implementation picks out the intermediate node through which the abnormality was performed. This is countered by tracking the intermediate nodes that are floating in the active route.

The novel strategy [10] spotlighted a credence based vehicle that can spot and extenuate the black hole intruder burls from the WSN. The faith rested play was proficient to fleck malicious nodal units, that too without forging any reconstructing in the routing lookup and without broaching accessory control caskets. In credence based scheme, for handcuffing, intermediate knobs are not statutory since the affair of diagnosis is actuated by the originator node itself.

Prioritizing security, this approach [11] revolves around detection as well as protection of the nodal environment.2 levels scheme, comprised of encryption and picking up malicious intruders using detection packet. The main implementations are elliptic curve cryptography and cuckoo search algorithm with detection packets. This work targets clustered WSN setup also trusted path is provided for secure routing. Reduction in length of routing path is another contribution to reduce energy consumption while data in transit. Objectives achieved include maximal accuracy, easy use, reliability, minimal energy loss and privacy .This work yields better life span along with throughput and a fall in packet drop ratio. As per results, this frame work adds to better performance with latency power of 20000 ms and through put reaching a high of 85% and maximum network span.

Another approach [12] followed same suit as the previous one [11]. It presented an improvised version of elliptic curve cryptography for data hiding to add security. Active trust plot is also updated along with data routing setup and data type checking while transmission. Work has also been done on increasing the privacy manifold by encrypting data prior to real routing. Results have outshined the previous similar work [11] in terms of security, reliable routing and network lifespan, not to forget energy consumption as well.

The design [13] focuses on making better the quality of health care wireless sensor network by discovery and segregation of Black Hole attack. The technology used here is name JENSEN-SHANON divergence estimation which joins hands with independent component analysis for the needful. This works by accumulation of physiological traits from biomedical sensors as well as sensor behavior namely trust energy, cooperative count. Reliance among the nodes is computed by independent probability distribution functions and mutual probability functions utilizing the above mentioned techniques. The result declares the culprit Black Hole node and the good normal node with precision. It not only quarantines the culprit nodes from the system but also updates the other nodes about its isolation. The achievements of the work include reliable data delivery, better detection rate, increment in packet delivery ratio, reduction in delay and minimum detection time of the attacker. Simulation covers metrics such as rate of diagnosis, time of recognition, fake alarm rates and packet conveyance ratio contemplating numerous diverse sensor nodes and data packets.

Another intrusion diagnosis technique [14] applies random forecast model for quarantine of the notorious enemy. In this model, decision trees are created which are to be added with data randomly. Decision split is also a part of process that chooses the features at random. This further decreases the correction between trees and calls for better output. F1 scores of attacks ensure the commendable performance which is 96 % for black hole in particular, otherwise follow respectively. This machine learning method stands out for topmost prediction precision, interpretability with conquering better generalizations implementing the strategies to the state of art.

A right combination of light weight neural network and specification rules is formulated for designing a full proof plot for catching malicious nodes [15]. The conversation that takes place between the sensor nodes and intrusion detection system is supervised as non-cooperating Bayesian game of two contenders. Also the amount of intrusion detection traffic in sensor network is brought down by the dominant factor of the plot, Bayesian Nash equilibrium which is monitored by a strategy following probabilistic. Further two diverse reputation update and expulsion techniques are inculcated to work in alignment and keep terrorized behavior among nodes at bay-namely Shapley value and Vickery- Clark grooves procedure. This actual execution takes place at three stages- sensor floor, segment of cluster head and base station zone for identifying the foreign element. At every level, a different strategy is compiled to. The sensor node level monitoring is confined to specification rules based taken up by intrusion detection system agents. The cluster head level is dealt with neural network based detection model. The base station level, keeps an eye on cluster heads for any symptom or gesture of maliciousness and consequently the infected cluster head is excluded from the network. The pros eye on high accuracy and detection rate are minimal energy consumption.

The proposal [16], integrates smart grid monitoring in addition to setting four different thresholds for packet drop ratio. Malicious nodes have been identified comparing trust and packet drop ratio for each cluster head. In case of malicious node found re-clustering operations for re-election of cluster heads on the basis of trust score. Out of the three thresholds(20%, 30%, 40% and 50%), the 50 percent one based on results has proved to reach system stability in early periods along with minimum number of re-clustering operations.

Authors in the paper [16], proposed a general approach for detection of five denials of service attacks, including Black hole attack by using proposed Energy prediction algorithm. They worked on network lifetime during which network works without losing energy and compute network lifetime using Network lifetime computation Algorithm. Energy consumption in case of attack and in normal case is compared and hence the attack is diagnosed.

Pertaining to energy utilization, a comparative analysis of diverse energy techniques in WSN has contributed to a conclusion that a mechanism must be devised to charge the sensor nodes like sun or wind instead of making use of scheduling for battery power conservation [17].

3. PROPOSED MODEL

The tendered apparatus entails the replication of blackhole invasions in non-cabled networks in NS2, under the speculation of only lone malignant invader nodal entity residing in the nexus. The discrete trace files were spawned for the scenarios overhead. These trace documents were put to train the energy rooted classifier in furtherance diagnosis of infected versus non-infected devices. Outcome of energy prototype takes the shape of Contingency listing depicting the association existing between diverse packet breeds (send (s), receive (r), forward (f) and drop (D)) and the knobs disposed in the nexus framework. The selfsame data is taken into view to discern whether a node is malignant or non-malignant. Sensing, processing, transmission or receiving data to achieve the mission of the field of interest, accompanies energy dissipation by sensors in a WSN setup [17].

3.1 *Mathematical model used for detection*

We portray X = $\{x_{1,}x_2\ldots\ldots\ldots,x_n\}$where X sample impersonates the node array in the wireless sensor inclined network setup; where n is the gross count of nodes.

The projection Y = $\{y_{1,}y_2\ldots\ldots\ldots,y_m\}$ where Y stages the assemblage of clean-cut countenance affiliated with each node. These cover send (s), receive (r), forward (f) and drop (d).
Apparent the gross count of enunciated lineaments (m) = 5

$$D = \sum_{j=1}^{m} \sum_{i=1}^{n} x_i y_j \qquad (1.1)$$

$X \in (x_{1,}x_{2,}\ldots\ldots,x_n)$; $Y \in (y_{1,}y_{2,}\ldots\ldots,y_m)$

Diagnosis (D) $=\{x_{1,}y_1+x_2y_1+x_3y_1+\ldots..+x_ny_m\}$ (1.2)

$Y \in \{0, 1\}$

0 = absence of mug
1 = presence of mug

Presumption that the lone visage with the maximum drop at the striker nodes and there is only solitary viral node lays foundation, then the above equations (1.2) will become

$$(D) = \{x_{1,}y_1+x_2y_1+x_3y_{1\ldots\ldots\ldots}\}$$
$$= \{x_{1,}y_1+x_2y_1+x_3y_1+\ldots..+x_ny_1\} \qquad (1.3)$$

The mathematical statement (1.1) will be curtailed to

$$D = \sum_{i=1}^{n} x_i\, y_j \qquad (1.4)$$

Consequently

$$D= \{x_1y_1+x_2y_1+x_3y_1+x_4y_1+x_5y_1+x_6y_1+x_7y_1\} \qquad (1.5)$$

Surrogating the figures of y_1 in the above equation where $Y \in \{0, 1\}$, inferring ‘drop d’ is on deck only at node ‘x_5’.

$$D=\{x_1*0+x_2*0+x_3*0+x_5*1+x_6*0+x_7*0\}$$
$$=\{x_5\}$$

Speculating about occurrence of drop at several nodes.

Let it stand at x_5 and x_3, n=7 and m=1;

$$D = \max(\textstyle\sum_{i=1}^{n} x_i\, y_1) \text{ where } Y \in \{0, 1\}$$
$$= \max \{x_1*0+x_2*0+x_3*0+x_5*1+x_6*0+x_7*0\}$$
$$= \max \{x_3,x_5\}$$
$$= \{x_5\}$$

3.2 *Simulation depiction*

In the implementation endeavors contemplatesa homogenous WSN which embodies network nodal entities with similar hardware and software setup as the real one. The replicating abode is presumed to inhabit symmetricity stating that a nodal unit can only converse with another similar bodyon the condition if Y can interact with X. Same operating characteristics are seen in every node in a network which comprises of power of transmission (Tx), height of antenna (h) and gain of antenna (g) all round the entire lifespan of the mesh. An outline of tactics of energy methodical target coverage in WSN has given another insight into decrement of energy by scheduling the set cover which is liable for target sensing as mentioned [18]. The topographical layout of each node can be secured with the aid of a GPS spotting system.Each node encapsulates the value of its identifier and topographical orientation in every message it gives out. The assumption follows that the messages which pursue exchanges in the network imply encryption to impart indispensible security to nexus. Theradio circulation further surmises to trail around with a well-expoundedmodel, which incorporates the Free Scope prototype and the Double-streak Ground Archetype [19]. This well elucidated schemespoint outhow the measuresof transmission power, gainedsignal brawn and gap between the spammerand the devisee are in a relationship. Also contrasting of various scheduling algorithms for nodes has been executed, pros and cons deeply assessed and results analyzed based on features as coverage order, connectivity order etc. which has let to scope for improvements in comparison thereby improving reliability with better coverage order and connectivity[20]

Atypical wireless nexus with sensor widgets is liable to fulfill following axioms in this proposed mechanism:

- Homogeneity: - In Toto employee nodes in the system compose alike silhouette.
- Undeviating behavior: - The network unit bodies possess preset stationed coordinates and they stay rooted to their location once deployed and set.
- Symmetricity:- The simulating ambit is presupposed to abide by conformity in which the X body is limited to interaction comprising Y unit node, provided Y is also willingly in a position to strike a communication facing X.

Ultimately, inference is reachedthat malicious entities are proficient of discharging blackhole strike only. The existenceof a malignant node is ascertained by the occurrence of large difference in the energy devouring by the nodes whilst sending, receiving and dropping of packets. In line with the raised situation,a message or a nodal entity can be adjudgedas dubious or non-dubious. The presentation contrasts and reveals battery utilization pattern in heuristics for lifetime amplification for WSN. Comparative assessment of QC-MCSC heuristic is done with prevalent heuristics to study battery performance style in WSN and how various battery models differ [21].

This part of the paper dispenses the information concerning dummy environment along with outcomes conjured. The Network Simulator2 is put to work to mock up the wireless sensor mesh systemhabitat with the intention to assess the facts and perform much needed analysis. The infrastructure of network is constructedcontaining the features as gathered in the table (I) pertaining to the pathway or the mechanism for drift beingcellular, the radiation is preset to be Two steak ground presuming that a prompt posted from a unit to some other prohibits from traversing in a linear line or an eccentric pavement and consequently hence via an echo in the deck, physiography employed is wireless concrete. The MAC kind inscription is applied tagging IEEE standard 802.11 analogous to every nodal unit. Diverse varieties of queues are applied to analyze the improvement of performance at the destination node. The priority based dribble appendage queue is effectuated where occurrence of trickling of facts packets is set to the rear end of the tool. Suitable choice of queue type at link node shows a decrement of packet fall and congestion [22].

Table 1: Simulation configuration

Sr no	Abbrevi-ation	Value	Description
1.	Chan	Channel/wireless Channel	Channel type
2.	Prop	Propagation /Two Ray Ground	Radio Propagation
3.	Netif	Phy/WirelessPhy	Network interface type
4.	Mac	Mac/802_11	MAC type
5.	Ifq	Queue/ Drop Tail/Priqueue	Interface Queue type
6.	II	LL	Link Layer Type
7.	Ant	Antenna/ Omni Antenna	Antenna model
8.	Fqlen	50	Max Packet in ifq
9.	Nn	16	Number of mobile nodes
10.	Rp	AODV	Routing Protocol
11.	X	800	X dimension of topography
12.	Y	541	Y dimension of topography
13.	Stop	100.0	Time of simulation end

This part of the paper dispenses the information concerning dummy environment along with outcomes conjured. The Network Simulator2 is put to work to mock up the wireless sensor mesh systemhabitat with the intention to assess the facts and perform much needed analysis. The infrastructure of network is constructedcontaining the features as gathered in the table (I) pertaining to the pathway or the mechanism for drift beingcellular, the radiation is preset to be Two steak ground presuming that a prompt posted from a unit to some other prohibits from traversing in a linear

line or an eccentric pavement and consequently hence via an echo in the deck, physiography employed is wireless concrete. The MAC kind inscription is applied tagging IEEE standard 802.11 analogous to every nodal unit. Diverse varieties of queues are applied to analyze the improvement of performance at the destination node. The priority based dribble appendage queue is effectuated where occurrence of trickling of facts packets is set to the rear end of the tool. Suitable choice of queue type at link node shows a decrement of packet fall and congestion [22].

Table 2: Nodes parameters during simulation

Sr no	Abbreviation	Value	Description
1.	Chan	Channel/wireless Channel	Channel type
2.	Prop	Propagation /Two Ray Ground	Radio Propagation
3.	Netif	Phy/WirelessPhy	Network interface type
4.	Mac	Mac/802_11	MAC type
5.	Ifq	Queue/Drop Tail/Priqueue	Interface Queue type
6.	II	LL	Link Layer Type
7.	Ant	Antenna/Omni Antenna	Antenna model
8.	Fqlen	50	Max Packet in ifq
9.	Nn	16	Number of mobile nodes
10.	Rp	AODV	Routing Protocol
11.	X	800	X dimension of topography
12.	Y	541	Y dimension of topography
13.	Stop	100.0	Time of simulation end

4. RESULTS

The overall number of packets generated and send by source node for a time period of 10 millisecond were 119.Under healthy case (the absence of BH), gross number of packets forwarded by intermediate nodes ‘9’& ‘10’ to the destination node’14’ were 119 ,with no fall of packets evident. The diseased case-blackhole pounce enumerates same number of packets was dispatched by node’0’ towards destination node’14’. The number of packets collected by intermediate nodes having number id ‘9’ & ‘10’ (blackhole) were 119. Not even a single packet was observed to be received by the destination node ‘14’. Indication of node ‘10’ conducting as a malicious black node attack node can be visualized in table (III).

Table 3: Total packets send, drop, forwarded andreceived against black hole and no black hole case.

CASE	SEND	DROP	FORWARDED BY 9	RECEIVED AT 10	RECEIVED AT 14
BLACK HOLE	119	119	119	119	0
NO BLACK HOLE	119	0	119	119	119

4.1Energy model

Energy Model is enacted in the Network Simulator as a node hallmark. The Energy prototype constitutes the degree of vigor in an ambulant host. The opening value of the level of valiant that the node embodies at the onset of the counterfeit is called initial Energy_. txPower_ and rxPower_ represent the energy utilized by each packet for transmission/reception. Also parameter values like initial Energy, txPower_ and rxPower_ arespecified in the energy model.

4.2 Energy analysis

After the clone energy is preserved in down flowing set-up in trace file

[Energy 998.999217 ei 1.000 es 0.000 et 0.000 er 0.001]

In overhead given syntax,initial name of trait is mentioned followed by its measure.

- energy: total remaining energy
- ei: energy ingestionwhile in IDLE state
- es: energy ingestionwhile in SLEEP state
- et: energy ingested while transmission of packets
- er: energy ingested while reception of packets

4.3 Performance measuring parameters

4.3.1 Minimum and maximum

Specimen maximum and specimen minimum are parameters that have been rigorously put to examine facts in statistics, also tagged as the man size observation and minuscule observation, and are the evaluates of the greatest and least elements of a pattern. The minimum and the maximum evaluates are the first and last disposition statistics (often designated as X (1) and X (n) respectively, for a trial set of n).

The sample maximum energy for the gross packets send in the existence of black hole attack was observed to be 3.4.The sample maximum energy for total packets send in the absence of black hole was also observed to be 3.4, indicating same amount of energy being consumed in the both cases. While maximum sample for energy against drop was observed to be 3.4 which was equal to the energy being consumed during receiving the packets in case of black hole and no black hole situation respectively. The above observation indicates malicious activity being seen in black hole scenario, while not in regular case. The similar observations related to maximum /minimum energy sample for both the cases can be seen in figure (1).

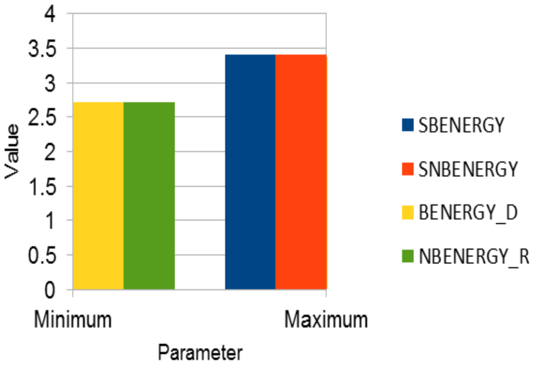

Figure 1: Showing total max/min energy against send /received and dropped packets in black hole and no black hole case.

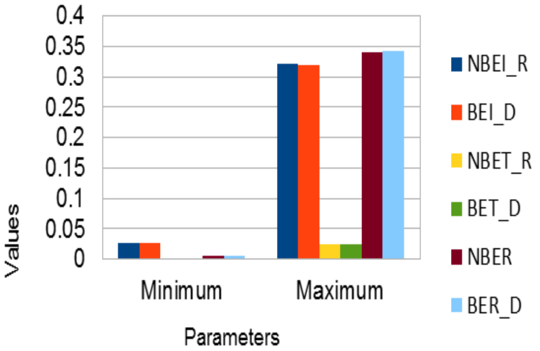

Figure 2: Showing total max/min idle, transmitting and receiving energy against received and dropped packets in blackhole and no blackhole case.

The maximum/minimum idle energy was observed to be 0.331/0.027 in case of no black hole while receiving the packets. The idle maximum/minimum energy was observed to be 0.32/0.326 in case of black hole while packets were not received but dropped instead. The transmitting max/min energy was observed to be 0.024/0.001 in case of black hole while receiving the packets. The transmitting max/min energy was observed to be 0.024/0.001 in case of black hole while packets were not receiving but dropped instead. The receiving max/min energy was observed to be 0.341/0.005 in case of no black hole while receiving the packets. The receiving max/min energy was observed to be 0.348/0.006 in case of black hole while packets were not received by dropped instead as shown in fig (2).

The above observations conclude the amount of energy at various states during receiving is almost equal to the amount of energy at various states during drop of packets. In other words receive energy (in no black hole) condition equals Drop energy in (black hole) condition.

4.3.2 Quartile 1 and quartile 3

The quartile records the expansion of energy evaluates overhead and low laying the mean by categorizing the dispensation into four teams. Q1 is the denotation taken up by first or lower quartile, and is the centre number that comes between the smallest energy value of the sample set and the median. Q2, the second in number quartile also is the median value.

Conveyed by this is that about 25% of the counts in the energy sample set falls beneath Q1 and about 75% resides aloft Q1. Q3 designated as the third quartile, is the estimates of median of the overlying half of the sample set. This also portrays evidently that about 75% of the numerals in the data specimen resides beneath Q3 and about 25% exists overhead Q3. The Q1/Q3 estimates observed in case of blackhole were 2.668601/ 3.116826 while similar values 2.66224/ 3.116564 were observed for sending energy in both the cases i.e. in the presence of blackhole and in the absence of blackhole. The Q1/Q3 values while packets were dropped, observed to be 2.862156/ 3.186825 in blackhole presence and 2.867261/ 3.186918 in the absence of blackhole while packets were received.

The similar energy score in both the cases against packets received and packets dropped indicates loss of energy while packets are dropped which equals the energy consumed during receiving of packets.

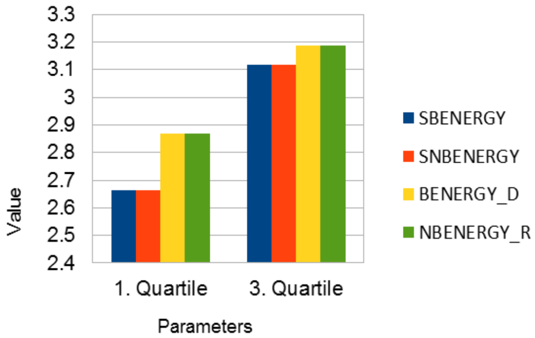

Figure 3: Showing comparison Q1/Q3 scores against send, received and dropped packets in blackhole and no blackhole case.

The Quartile (1) and Quartile (3) scores observed for idle, transmitted and receiving energy were 0.107/ 0.2515, 0.0076/ 0.019 and 0.0995/ 0.2035 respectively in the absence of blackhole against packets received as shown in fig (3).The Quartile (1) and Quartile (3) scores observed for idle, transmitting and receiving energy were 0.106/ 0.2505, 0.0075/ 0.019 and 0.0945/ 0.2635 respectively in the presence of blackhole against packets dropped as shown in fig (4).

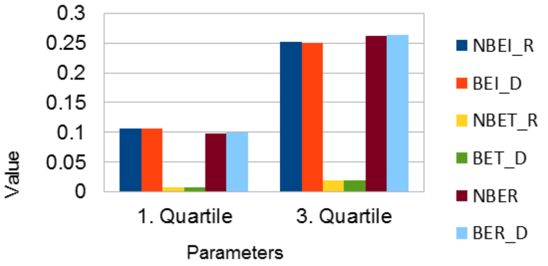

Figure 4: Showing Q1/Q3 scores for idle, transmitting and receiving energy consumed against received and dropped packets in blackhole and no blackhole case.

5. CONCLUSION

The mechanism taking game proves to fulfil its promised task. Energy patterns show variations in different aspects of the system, paving way to effectuate analysis of the results putting a stamp to the diagnosis. The moment performing the traverse of packets from source to sink node, outcomes in a decline in energy as observed with respect to time is manifested in fig (1). The manifested fall in the vigour is an evident attestation of the residence of certain dubious malignant ventures whilst the relay transit. The energy consumption volume for remaining nodes verifiesthese nodal bodies are either infected or not resident to the road to the destination. It can be very well speculated that no decline in the energy occurs in lieu to time incurred for the packets itinerary from originator node to terminus sink unit as evident in fig (2). The no drizzle state in the plot distinctly renders the non-appearance of any viralactivity during the locomotion.

Since energy consumption increment observed at node (10) and the node is also in the route to the destination indicates being blackhole. The diverse implements and algorithms put to use show a roadmap to smooth detection.

REFERENCES

[1] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensing element networks,” IEEE Communications Magazine, (2002), vol. 40, no. 8, pp. 102–114.

[2] T. Arampatzis, J. Lygeros, and S. Manesis, “A Survey of Applications of Wireless sensing elements and Wireless Sensor Networks,” in Proceedings of the 2005 IEEE International conference on, Mediterrean Conference on management and Automation Intelligent management, (2005), June, pp.719–724.

[3] R. Johnstone, D. Caputo, U. Cella, A. Gandelli, C. Alippi, F. Grimaccia, N. Haritos, and R. E. Zich, “Smart Environmental Measurement and Analysis Technologies

(SEMAT): Wireless sensor networks in the marine environment," presented at the Wireless Sensor and Actuator Network Research on Opposite Sides of the Globe (SENSEI), 2008.

[4] Sunita Gupta., K.C. Roy, Dinesh Goyal, Sakar Gupta.,"A Novel Energy Efficient connected Target Coverage heuristic In WSN", International Journal of Computer Science and Information security (IJCSIS),(2016), Vol. 14, No. 4.

[5] J. M. Kahn, R. H. Katz, and K. S. J. Pister. "Next century challenges: Mobile networking for "smart dust". In International Conference on Mobile Computing and Networking (MOBICOM), (1999) pages 271–278, 1999.

[6] Abderrahmane Baadache, Ali Belmehdi "Avoiding Black-Hole & Cooperative-BlackHole Attacks : in Wireless-Ad-hoc-Networks" (IJCSIS) International journal of Computer Science and Information Security, (2010), Vol. 7, No.1.

[7] J. M. Kahn, R. H. Katz, and Kristofer S. J. Pister " Rising challenges, Mobile Networking for 'Smart Dust", Journal of Communications and Networks, (2000), 2(3):188–196.

[8] Khemariya, Neelam, and Ajay Khuntetha. "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs." International Journal of Computer Applications, (2013), vol. 66, no.18.

[9] Tran Hoang Hai, Eui-Nam Huh "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge", proceedings of the Seventh IEEE International Symposium on Network Computing and Applications, (2008), pages 325-331.

[10] Banerjee, Subhashis, Mousumi Sardar, and Koushik Majumder."AODV Based Black-Hole Attack Mitigation in MANET", In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) (2013), Springer International Publishing, (2014) pp.345-352.

[11] Deepak C. Mehetre , S. Emalda Roslin, Sanjeev J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust" Springer Science+Business Media, LLC, part of Springer Nature ,Springer US, cluster computing , (2018), pp 1-16.

[12] M. Shinde and D. C. Mehetre, "Black Hole and Selective Forwarding Attack Detection and interference in WSN," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, (2017), IEEE Xplore,(2018), pp. 1-6.

[13] A. John Clement Sunder and A. Shanmugam, "Jensen–Shannon Divergence Based Independent Component Analysis to Detect and Prevent Black Hole Attacks in Healthcare WSN", Springer Science+Business Media, LLC, part of Springer Nature (2019), A. Wireless Pers Commun (2019).

[14] Thi-Thu-Huong Le, Taehwan Park, Dongkeun Cho and Howon Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks", Tenth International Conference on Ubiquitous and Future Networks (ICUFN) (2018), IEEE Xplore, August (2018).

[15] Basant Subba, Santosh Biswas and Sushanta Karmakar, "Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks", Springer Science+Business Media, LLC, part of Springer Nature (2018), International Journal of Wireless data Networks, (2018), volume 25, Issue 4, pp 399-421.

[16] Safa Otoum, Burak Kantarci and Hussein T. Mouftah, "Hierarchical Trust based, Black hole detection in WSN based Smart Grids" IEEE,International conference on communications, Paris, France, (2017), pp 1-6.

[17] Sunita Gupta., K.C. Roy," Comparison of Different Energy Minimization techniques in a wireless sensor network", International Journal of Computer Applications, (2013), (0975-8887) 75 (18).

[18] Sunita Gupta, K.C. Roy," Energy Efficient target Coverage issues in wireless sensor network", International Journal of Computer Organization Trends 1 (3)(2011), ISSN:2249-2593.

[19] T. S. Rappaport, "Wireless communications: principles and practice", tiro Hall, second edition, 2002.

[20] Sunita Gupta, K.C. Roy," Comparison of Sensor node Scheduling algorithms in wireless sensor networks", International Research Journal of Engineering and Technology (IRJEI) 02(06) (2015), e-ISSN:2395-0056.

[21] Sunita Gupta, Sakar Gupta," Comparative Analysis of Energy Consumption in Sensor Node scheduling Heuristics in wireless sensor networks", Springer Nature Singapore Pte Ltd. (2019).

[22] R. Bahl, R. Kumar and J. P. Singh, "Comparison of buffering in Manhattan Street Network in NS2," Communication Systems, Networks and Applications (ICCSNA), (2010) Second International Conference on, Hong Kong, (2010), pp. 441-443.