International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8, Issue-9S, July 2019

Method & Implementation of Fault Detection & Prevention Attack in WSN

Deepak Dhadwal, Vinay Bhatia, PN Hrisheekesha

Abstract—***In WSNs, a major problem is the assaults on nodes or more sinks. In any case, this information rate is obliged by the accessible vitality at every hub just as connection limit. After sending, some sensor hubs may obstruct the measure of information that land at a sink due to their low vitality reaping rate. In this work, the fundamental objective is to recognize and detect blackhole attack in WSN. These assaults may decrease the exhibition of framework. In this work, it gives deficiency dealing with in system and can improve execution. Likewise stream can improve by utilization of advancement calculation in the system. The proposed framework improves vitality just as stream of framework. All recreations are done in simulation tool. The proposed system is executed with MATLAB. The work has increased the maximum flow of information to 30% with increase in degree of nodes.***

Index Terms- Routing in WSN ,Max Flow,Tabusearch,Routing in WSN

I. INTRODUCTION

Remote Sensor System have delighted in impressive enthusiasm from the examination network because of their changed applications and one of a kind difficulties. They have discovered applications in military use for "adversary following, front line observation, and target arrangement" just as different applications including traffic checking, cross-fringe penetration location, military surveillance, environment checking, and so forth. Because of the low assembling expenses of WSN hubs, they can be sent in huge numbers yielding difficulties in system the board, for example, directing, topology control, and information the executives conventions. These difficulties are just confused by extreme vitality requirements and the innately problematic nature of remote correspondences which have yielded work in expanding system productivity and enlarging conventions with shifting degrees of adaptation to non-critical failure. This work explicitly addresses the utilization of adaptation to internal failure to improve the total proficiency of the WSN.

A remote sensor arrange (WSN) is a self-sorted out arrangement of little, autonomous, ease, low fueled and remotely imparting hubs conveyed over a huge territory with one or perhaps progressively incredible sink hubs gathering readings of sensor hubs and, may deal with an assortment of detecting, inciting, imparting, signal preparing, calculation, and correspondence undertakings, sent without perpetual system foundation and in situations with restricted or no human openness. The sink fills in as the door between the client application and the sensor organize.

For the most part, activity of WSN includes correspondence between sensor hub and base station. The sensor hub detects condition, play out some calculation (whenever required) and report accumulated data to the base station. In this, the nodes are communicated with base station when some trigger happens or some event occurred.

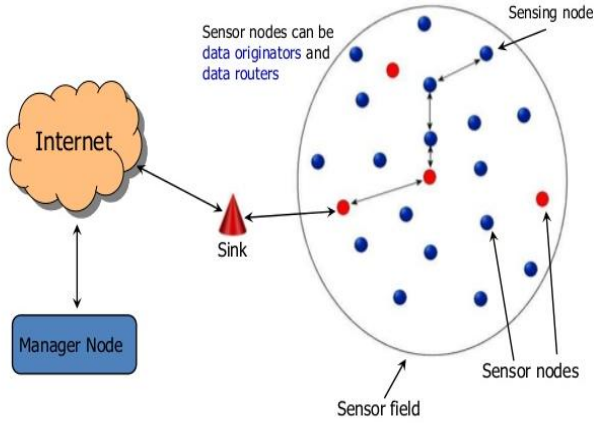

Figure 1: WSN Architecture [1]

Convenience Offered by Wireless Networks

Mobility

This is one of the conspicuous points of interest of the remote systems. Portable clients can associate with the current systems while wandering unreservedly and getting a charge out of autonomy.

Simplicity

We can make an interpretation of straightforwardness into quickadvancement. It is anything but difficult to introduce a remote framework, contrasted with a wired system.

Flexibility

Remote system inclusion region can achieve where wire can't go. It is extremely helpful for moving vehicles or for the spots where running link is beyond the realm of

Revised Manuscript Received on June 15, 2019

Dr. Deepak Dhadwal,ECE Departement, CGC Landran, India
Dr. Vinay Bhatia, ECE Departement, CGC Landran, India
Dr. PN Hrisheekesha,CampusDirector,CGCLandran, India

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

imagination like chronicled structures.

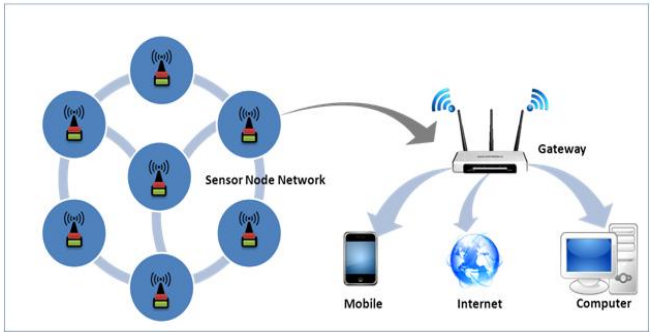

Figure 2: Wireless Sensor Network [1]

This work is presented as follows. In area second, it speaks to real difficulties in WSN organize. In Section III, It characterizes the different directing conventions. Area IV characterizes the proposed framework. The aftereffects of proposed framework is characterized in segment V. At last, end is clarified in Section VI.

II. LITERATURE REVIEW

Tengjiao He et al. (2016) [1], exhibited a novel methodology whereby the plan to "overhaul" the reviving rate of a limited number of "bottleneck" hubs utilizing purported Auxiliary Chargers (ACs) furnished with Wireless Power Transfer (WPT) ability. It figured a Mixed Integer Linear Program (MILP) for the NP-difficult issue nearby and proposed three novel answers for spot ACs: (I) Path, which specially updates hubs on the most limited way among ways from sources to sinks, (ii) Tabu, a meta-heuristic that first uses Path as the underlying arrangement. It at that point scanned for a neighbouring arrangement that yields a higher max stream rate.

Gurbinder Singh Brar et al., 2016 [2] proposed a novel and proficient strategy to recognize the wormhole assault without equipment hardware or requiring much data about WSN. The proposed strategy utilized a moving normal (MA) pointer, which has been regularly utilized in money related fields, to apply to neighbors of sensor hubs; it turns into a dynamic recognition marker of the quantity of neighbor hubs. Since the mixes are too various to even think about arranging, it used a Quantum-propelled Tabu Search (QTS) calculation. The main performance parameters were throughput, energy and computation time. The computation model was assessed.

Jaspreet Kaur et al., (2015) [3] proposed another information re configurable strategy which has improved the exhibition of the WSNs. This helped to improve maximum flow in network by improving energy of system. This procedure was driven by the sensors whose upstream hubs bomb because of harms. In particular, the areas of fizzled sensors on previous courses were utilized to evaluate the range of the harm and a portion of the sensors are migrated to such areas to restore the courses with the sink hub. Migration on such previous courses is performed so that the development overhead on sensors was additionally limited.

Meng-Hsiu Jao et. al (2015) [4] proposed a novel and proficient strategy to recognize the wormhole assault without equipment hardware or requiring much data about WSN. The proposed strategy utilized a moving normal (MA) pointer, which has been regularly utilized in money related fields, to apply to neighbors of sensor hubs; it turns into a dynamic recognition marker of the quantity of neighbor hubs. Since the mixes are too various to even think about arranging, it used a Quantum-propelled Tabu Search (QTS) calculation. This calculation was productive and compelling in finding the perfect mix of identification markers to identify wormhole assaults in various situations. The reenactment result demonstrated our strategy is natural and effectively identifies wormhole.

Madhu. B.M et. al (2014) [5] proposed an improved directing convention to decrease the power utilization of the installed hub by lessening the calculation overhead and information steering through less vitality devouring course through sensor hubs of intrigue. Remote sensor hubs must use the insignificant conceivable vitality while working over a wide scope of working situations. Because of the huge number of remote sensor hubs that might be conveyed and the long framework lifetimes required, supplanting the battery isn't an alternative. The information transmission and gathering between the remote sensor hubs and the sink and source hubs adds to significant vitality utilization, which should be taken care of with consideraion.

N. Gaur et. al (2014) [6] suggested that remote work organize is a circulated multi-bounce handing-off system. In this paper, they proposed a Load-mindful Non-Persistent little world long connection Routing calculation for little world remote work systems to accomplish lower normal transmission way length for information exchange sessions among a lot of source-hub and goal hub matches in the system. LNPR utilized burden adjusting system to all the more likely convey the system traffic among the typical connections and the non-relentless long-interfaces in the little world remote work systems for productive utilization of long-joins which are valuable information transmission ways in the system.

Shih et. al (2013) [7] proposed an issue hub recuperation calculation to upgrade the lifetime of a remote sensor arrange when a portion of the sensor hubs shut down. The calculation depended on the evaluation dispersion calculation joined with the hereditary calculation. The calculation could result in less substitutions of sensor hubs and more reused directing ways. In this recreation, the proposed calculation expanded the quantity of dynamic hubs up to 8.7 occasions, diminished the rate of information misfortune by around 98.8%, and decreased the rate of vitality utilization by roughly 31.1%.

P. Chanak et. al (2013) [8] revealed a circulated multipath adaptation to non-critical failure steering plan for remote sensor organize (DFTR). The multipath adaptation to internal failure steering gave better strength to different blames in remote sensor organize (WSN). Be that as it may, the multipath adaptation to non-critical failure directing had endured by two issues with respect to the steering technique structure. The primary issue was that the traffic overhead turns out to be high. In this, a disseminated multipath shortcoming tolerant directing plan had created to handle these issues in WSN. Compelling size bunch arrangement was utilized to anticipate traffic over head and vitality gap.

A. Abbasi et. al (2013) [9] recommended that in remote sensor-on-screen character

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

systems, sensors test their environment and forward their information to entertainer hubs. On-screen characters cooperatively react to accomplish predefined application mission. Since entertainers need to arrange their task, it was important to keep up a firmly associated system topology consistently. In addition, the length of the between entertainer correspondence ways might be obliged to meet inactivity necessities. In any case, a disappointment of an entertainer may make the system parcel into disjoint squares and would, therefore, damage such an availability objective. This paper beats these weaknesses and exhibited a Least-Disruptive topology Repair (LeDiR) calculation. LeDiR depends on the nearby perspective on a hub about the system to devise a recuperation plan that migrates minimal number of hubs and guarantees that no way between any pair of hubs is broadened.

K. Akkaya et. al (2013) [10] exhibited a circulated segment recognition calculation which rapidly makes the sensors mindful of the parceling in the system. This procedure was driven by the sensors whose upstream hubs bomb because of harms. In particular, the areas of fizzled sensors on previous courses were utilized to evaluate the range of the harm and a portion of the sensors are migrated to such areas to restore the courses with the sink hub. Migration on such previous courses is performed so that the development overhead on sensors was additionally limited. Our proposed methodology exclusively relies upon the nearby data to guarantee automaticity, practicality and adaptability.

N. Jabeur et. al (2013) [11] proposed another scientific classification (PLMS) which characterizes openings into sort bunches as indicated by the reason for abnormality. They examined the impacts of gaps on the sensor organize. At long last, they study the diverse remedial methodologies (counteractive action, identification, fixing, evasion). The four distinct orders displayed are identified with various parts of sensor openings. They think about sensor gaps from a reason impact arrangement point of view, it will concentrate on the reason based classification that it named Physical/ Logical/ Malicious/ Semantic (PLMS) scientific categorization.

J. Kullaa et. al (2013) [12] recommended that in this examination, the goal was to distinguish, recognize, and evaluate a sensor shortcoming utilizing the auxiliary reaction information estimated with the sensor organize. Seven diverse sensor deficiency types were researched and displayed: predisposition, increase, floating, accuracy corruption, complete disappointment, clamor, and steady with commotion. The sensor deficiency is recognized and evaluated utilizing the different speculation tests using the summed up probability proportion (GLR). The proposed methodology was tentatively checked with a variety of accelerometer amassed on a wooden scaffold. Distinctive sensor shortcomings were recreated by altering a solitary sensor. The strategy had the option to recognize a sensor flaw, distinguish and right the broken sensor, just as distinguish and measure the deficiency type.

III. DIFFRENT ATTACKS AND VARIOUS ROUTING PROTOCOLS

1. Types of Attacks

Passive Eavesdropping

An aggressor may tune in to remote system to comprehend which is happening in this system. It initially tunes in to control communication to construe the system geometry to see how hubs are found or are speaking with another. Along these lines, it can accumulate insightful data about the system before assaulting. It might likewise tune in to the data that is transmitted utilizing encryption in spite of the fact that it ought to be private having a place with upper cover applications. Listening in is additionally a danger to area security [13]. An unapproved hub can see a remote system that exists inside a land region, just by identifying radio sign. To battle this, traffic designing methods have been created.

Selective Existence (Selfish Nodes)

Thenoxieous hub which is otherwise called narrow minded hub and which isn't taking part in the system tasks, utilize the system for its preferred position to upgrade execution and spare its very own assets, for example, control. To accomplish that, narrow minded hub advances its reality at whatever point individual expense is included. Hence these egotistical hub practices are known as particular presence assaults. [14]. At the point when a narrow minded hub needs to begin an association with another hub, it plays out a course revelation and after that sends the vital bundles. At the point when the hub no longer needs to utilize the system, it comes back to the "quiet mode" After some time, neighbouring hubs discredit their own course sections to this hub and childish hub ends up undetectable on the system.

Gray Hole Attack (Routing Misbehaviour)

Gray hole assaults is a functioning assault type, that can cause message dropping or malfunctioning. Assaulting hub initially consents to advance parcels and after that neglects to do as such[15]. At first the hub acts effectively and replays genuine packet messages to hubs that start RREQ message. Along these lines, it assumes control over the transport bundles. A short time later, the hub just drops the parcels to dispatch a disavowal of administration assault.

Black Hole Attack

Malevolent hub assaults all RREQ messages along these lines and assumes control over all courses. Along these lines all parcels are sent to a moment that they are not sending anyplace. This is known as a dark opening similar to genuine significance which swallows all items and matter. To succeed a dark gap assault, pernicious hub ought to be situated at the focal point of the remote system.

2. *Operation Based Routing Protocols*

Energy-Aware WSN Routing Protocol

This Routing is a responsive convention to build lifetime of the system. This convention keeps up a lot of ways. The upkeep and choice relies upon a specific likelihood, which transfers on how low the vitality

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

utilization of every way can be accomplished[16]. The convention makes steering tables about the ways as indicated by the expenses. Restricted flooding is performed by the goal hub to keep up the ways alive.

IV. DESCRIPTION OF PROPOSED SYSTEM

Information preparing is a noteworthy part in the task of remote sensor systems. Consequently, directing strategies utilize various information handling procedures. By and large, sensor hubs will participate with one another in preparing various information overwhelmed in the system territory. In this work, it presents information stream steering under different assaults with most brief way. It additionally covers vitality streamlining with bunching of hubs. Deficiency discovery is the principal period of issue the board, where a surprising disappointment ought to be appropriately recognized. Appropriated approach empowers the idea of nearby basic leadership, which equitably disperses shortcoming the board into the system. Its objective is to enable a hub to settle on specific dimensions of choice before speaking with the focal hub[17].

As displayed by writing, system bombs because of the consumption of vitality, send-off hub portioned by staying reasonable system hubs. With the current convention, at the elimination of the system (when the sink is disengaged from the staying live system hubs), the rest of the vitality is adequately overcome with zero effectiveness since it is never again accessible for valuable work which discredits the reason that their methodology limits vitality utilization inside the system[18].

With the current convention, at the termination of the system (when the sink is detached from the staying live system hubs), the rest of the vitality is adequately overcome with zero productivity since it is never again accessible for helpful work which refutes the reason that their methodology limits vitality utilization inside the system. In this work, we have endeavoured to assess the impacts of the Black Hole assaults in the remote Ad-hoc Networks. To accomplish this we have re-enacted the remote impromptu system situations which incorporates Black Hole hub utilizing MATLAB program. To mimic the Black Hole hub in a remote specially appointed system we have actualized another convention that drops information bundles in the wake of drawing in them to itself[19].

Tabu inquiry is a versatile hunt strategy, utilizing the best improvement nearby pursuit as the fundamental fixing. By permitting transitory arrangement corruption, tabu inquiry maintains a strategic distance from the pursuit procedure being caught into the nearby ideal. Two components, the momentary memory and long haul memory, can be connected to monitor properties of recently visited arrangements and guide the tabu hunt process. One of the primary segments of Tabu Search is its utilization of versatile memory, which makes a progressively adaptable hunt conduct. Memory-based procedures are thusly the sign of tabu pursuit approaches, established on a mission for "coordinating standards," by which elective types of memory are suitably joined with powerful systems for misusing them. A tale finding is that such standards are at times adequately strong to yield successful critical thinking conduct in their own right, with unimportant dependence on memory.

The subject of WSN continues creating as a ready research zone. Attempts constantly hope to vanquish the complexities of strong, or even issue tolerant, correspondences in enormous remote frameworks. In this work, the effects of the adaptable sink in the a huge segment of the essentialness profitable shows have been ignored. In this work, the standard target is to recognize and keep away from dim opening attack in WSN. To finish a dim hole strike, vindictive center point believes that neighboringcenters will send RREQ messages. The confinement steps pursued by utilizing Tabu Search Algorithm are that it takes the aftereffects of Mobile Anchor Positioning as its info. The consequences of MAP, giving the rough arrangement of the area of every sensor at each predetermined time occasion is given as the contribution to the post improvement strategy.

Malignant center point strikes all RREQ messages thusly and expect command over all courses. In like manner all bundles are sent to a minute that they are not sending wherever. This is known as a dull opening much equivalent to certifiable significance which swallows all articles and matter. To succeed a dull opening attack, vindictive center point should be arranged at the point of convergence of the remote framework. In case harmful center camouflages false RREP message as if it begins from another harmed individual center point as opposed to itself, all messages will be sent to the deplorable setback center point. By doing this, shocking setback center point should process each and every moving toward message and is presented to an absence of rest attack.

The main problem in this work is the attack of black hole in network that can cause harm to the system. Due to this, it can affect the performance of system. In any case, this data rate is obliged by the available imperativeness at each center point similarly as association limit. After association, some sensor center points may block the proportion of data that connect at a sink in perspective on their low imperativeness gathering rate. The Proposed show, identified with the depiction of the remainder of the framework essentialness, attempts to widen the profitable presence of the framework, growing capability to the extent imperativeness utilized, compose cost and max stream of framework[20].

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

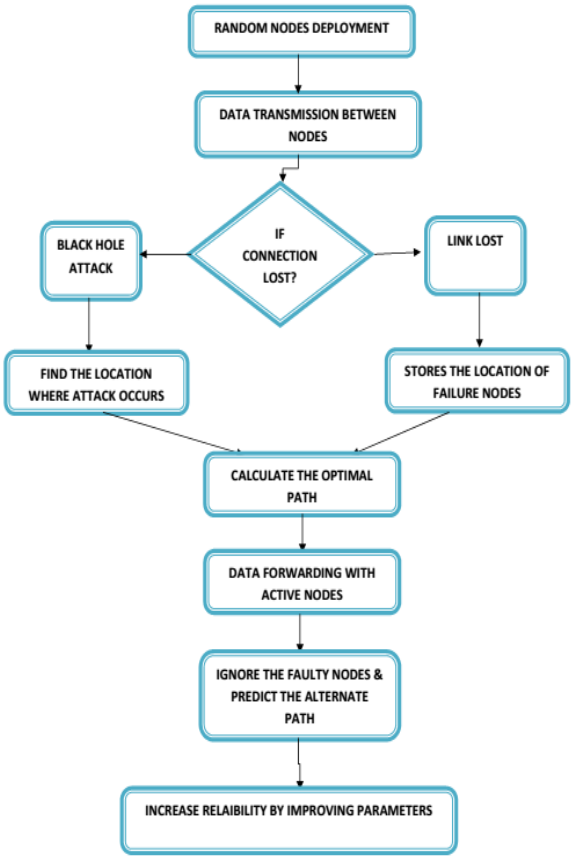

Figure 3: Proposed Flow Chart of System

The confinement steps pursued by utilizing Tabu Search Algorithm are that it takes the aftereffects of Mobile Anchor Positioning as its info. The consequences of MAP, giving the rough arrangement of the area of every sensor at each predetermined time occasion is given as the contribution to the post improvement strategy. At any emphasis it needs to locate another arrangement by making nearby developments over the present arrangement. The conceivable arrangement of a hub which was anticipated by MAP calculation is kept up in a tabu rundown. The normal separation of neighbour hubs of the comparing hubs are determined. The distinction between the area and the normal separation of the hub are determined. In the event that the arrangement is not exactly the normal esteem, at that point that esteem is considered as a best arrangement.

The "following arrangement" is the best among all (or a subset of) potential arrangements in the area so as to complete the investigation procedure, the as of late visited arrangements are maintained a strategic distance from. Tabu rundown is kept up. Along these lines once an answer is visited, the development from which it was acquired is considered as tabu. N(ω) will change along the investigation, so in a specific sense dynamic neighbourhood is contrasted with the past nearby pursuit calculations where stays static. Normally there are two sorts of tabu records, a long haul memory and transient memory. Long haul memory keeps up the history through all the investigation procedure all in all and a transient memory is to keep the most as of late visited tabu developments. A development with a tabu status (tabu development) is maintained a strategic distance from to be connected, except if it fulfils certain desire criteria. This means to abstain from falling into nearby optima. Tabu rundown estimate is fixed before the hand every component of the rundown has a place with it for various cycles limited by given greatest and least qualities. Rehash the cycles until the halting criteria are met.

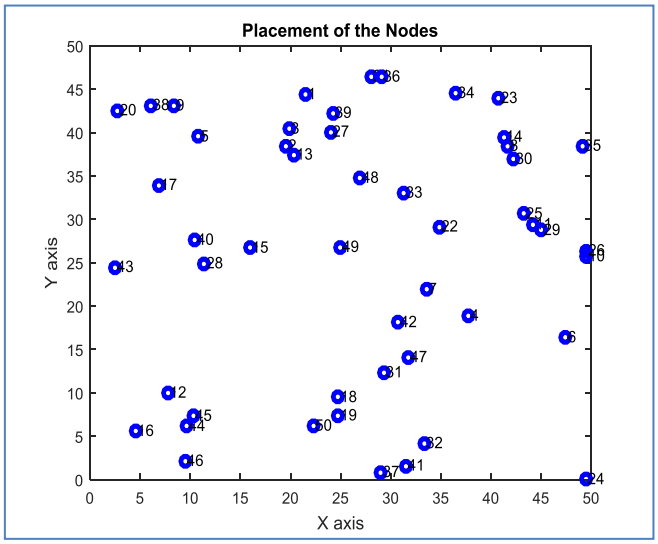

Figure 4: Nodes Placement in Network

V. RESULTS & DISCUSSION

The fundamental goal is to distinguish and deal with dark opening assault in system. The scattering vitality in correspondence process is the fundamental variables we have to limit. Moreover, the quantity of CHs can factor into the goal work. Less CHs result in more prominent vitality proficiency and higher CHs expend more vitality as CHs channel more power than non-group heads. Following are the usage results for the situation. This work contains 50 nodes for simulation and also provides random location in network. All nodes have a battery and sensing device that helps to communicate with each other.

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

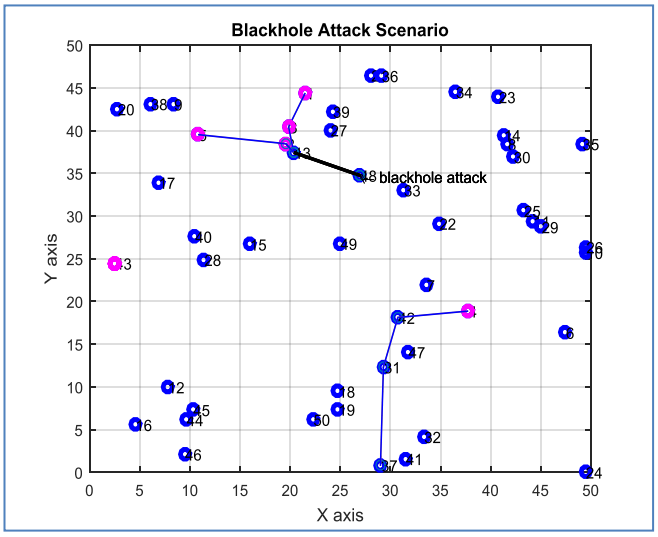

Figure 5: Black hole Attack in Network

Every sensor has a number with it that helps to find faulty node in network. It will be utilized to address any sensor all through the procedure. Here we take huge number of sensors so that proposed plan will assess effectively. The data of the considerable number of hubs will be update to single hubs to which we accept as a cell supervisor. This arrangement is a normal capacity of organize factors characterized in the vectors. They are arbitrary in nature. No two hubs cover one another. Here we take the 50*50 m2 territory for arrangement of sensor hubs. The hubs are conveying and connections gets flopped because of loss of vitality and it don't achieve its goal (appeared in fig 4). In dark gap assault, a noxious hub publicizes itself as the most brief way and pulls in every one of the information traffic towards itself. It assimilates all bundles without transmitting them to the goal. The source hub starts the course revelation process by communicating Route Request (RREQ) bundle to its neighbour. The whole neighbour who gets the RREQ advances it further towards the goal by including their location with it.

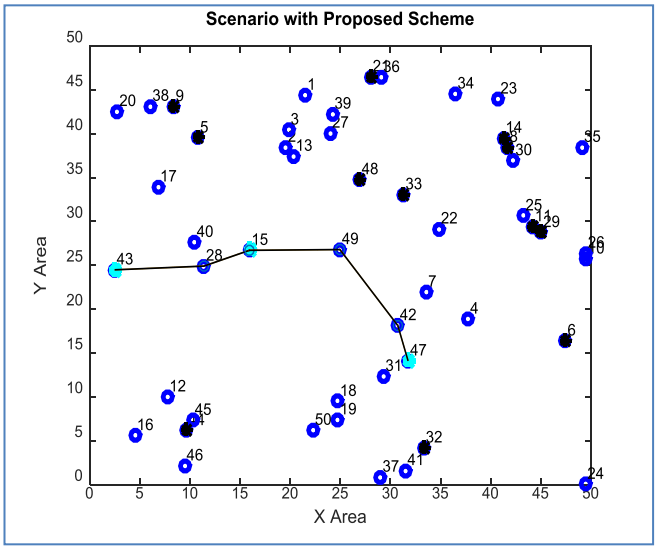

Figure 6: Scenario with Proposed Scheme in Network

In this work, the fundamental objective is to develop a quick tabu scan calculation for registering arrangements of good quality for huge occasions of the minmax issue in WSN. In proposed plot, hubs with low vitality gets defective and appeared black shading in figure 5. As information gets transmitted from sender to beneficiary, it broken hub comes in the way of information transmitter hub, hub may anticipate the substitute way from that and pick interchange most brief way with the goal that it can achieve the goal effectively. Be that as it may, cost may gets decreased and consequently execution is improved by utilization of tabu hunt. System cost is characterized as far as burden esteem. Lower the cost methods organize is streamlined and execution is better. Along these lines, Tabu inquiry streamline the system by refreshing the areas of hubs and furthermore with the assistance of separation from past hubs as appeared in fig 7.

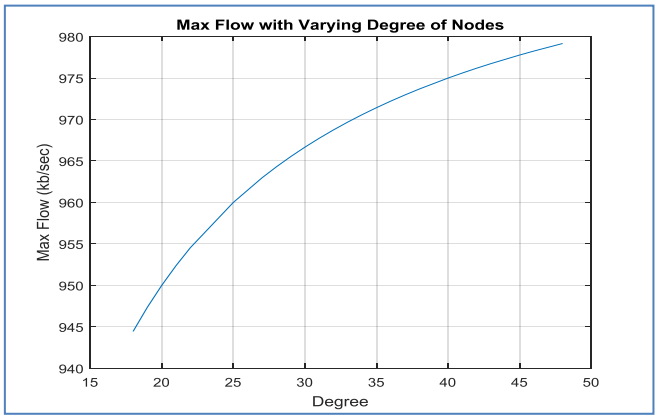

Figure 7: Performance of Max Flow in Network

VI. CONCLUSION

This work provides the concept of blackhole attack in WSN that can affect the performance of system by generating faulty nodes. These nodes affect the energy level of nodes as well as the network lifetime. Due to this, it presents a faulty node detection and prevention method to handle these types of hubs. By current convention, at the termination of the system, the rest of the vitality is adequately overwhelmed by zero productivity since it is never again accessible for helpful work which invalidates the reason that their methodology limits vitality utilization inside the system. In this, the rule concern is to recognize and turn away dim opening attack in WSN. In this work, the standard goal is to construct a figuring for handling plans so execution may improve. The outcomes demonstrates the improvement in stream of system just as in progress of vitality of hubs.The results are presented and useful in terms of network lifetime and packetloss. The proposed results shows the improvement as compared to actual results in terms of path length and packet loss.

REFFERENCES

[1] D. Linden and T. B. Reddy, 2002,Handbook of Batteries. McGraw-Hill Professional: New York.

[2] S. Davis, 2004, Basics of Design: Battery Power

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Management. Supplement to Electronic Design.
[3] Y. Cheng, D.P. Agrawal, 2006, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks", Elsevier Ad Hoc Networks, pp.35-48.
[4] Wenqing Cheng, ZhiqiangXiong, Wei Liu, 2006, "Hybrid Solution: A FEC Algorithm for Fault Tolerant Routing in Sensor Networks", IEEE International Conference on Communications and Networks, China, pp.0463-0467.
[5] ZhiqiangXiong, Zongkai Yang, Wei Liu, Zhen Feng, 2006, "A Lightweight FEC Algorithm for Fault Tolerant Routing in Wireless Sensor Networks", IEEE International Conference on Wireless Communications, Networking and Mobile Computing, pp 1-4.
[6] S. Ozdemira, Y. Xiao, 2008, "Secure data aggregation in wireless sensor networks: A comprehensive overview", Elsevier Computer Networks, pp. 202-2037.
[7] L.T Nguyen, X.Defago, R.Beuran, Y.Shinoda, 2008, "An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", IEEE International Symposium on Wireless Communication Systems, pp. 568-572.
[8] W.H Liao, H-H Wang, 2008, "An asynchronous MAC protocol for wireless sensor networks", Elsevier Journal of Network and Computer Applications, pp. 807–820.
[9] J. Zhua, K.L Hunga, B. Bensaoua, F.N Abdesselam, 2008, "Rate-lifetime tradeoff for reliable communication in wireless sensor networks", Elsevier Computer Networks, pp. 25-43.
[10] Lan Tien Nguyen, Xavier Defago, 2008, "An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", IEEE International Symposium on Wireless Communications Systems, pp.568-572.
[11] Tsai-Wei Wu and Hung-Yun Hsieh, 2008, "Interworking Wireless Mesh Networks: Performance Characterization and Perspectives", IEEE Global Telecommunications Conference, pp.4846-4851.
[12] Zhang Lili, Wang Huibin, Xu Lizhong, 2009, "Fault Tolerance and Transmission Delay In Wireless Mesh Networks", IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 193-196.
[13] Chuang Wang, Taiming Feng, Jinsook Kim, 2009, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Social Conference on Sensors, Mesh and Ad hoc Communication and Networks,pp.2908-2916.
[14] Anna Abbagnale, Emanuele Cipollone, 2009, "A case study for evaluating IEEE 802.15.4 wireless sensor network formation with mobile sinks", IEEE International Conference on Communications, pp. 3435-3439.
[15] Che-Aron, Z., Al-Khateeb, 2010, "An Enhancement of Fault-Tolerant Routing Protocol for Wireless Sensor Network", International Conference on Computer and Communication Engineering (ICCCE), pp.6235-6240.
[16] Dario Bruneo and Marco Scarpa, 2010, "Adaptive Swarm Intelligence Routing Algorithms for WSN in a Changing Environment", IEEE Sensors Conference, pp.1813-1818.
[17] Preetam Ghosh, Michael Mayo, VijenderChaitankar, 2011, "Principles of Genomic Robustness Inspire Fault-Tolerant WSN Topologies: a Network Science Based Case Study", Seventh IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, pp.160-165.
[18] Z Jun, C. Xiang-guang, 2011, "The application of multi-path fault tolerant algorithm in WSN nodes", IEEE International Conferences on Artificial Intelligence, Management Science & Electronic Commerce, pp. 7323-7326.
[19] L. Karim, N. Nasser, 2012, "Reliable location-aware routing protocol for mobile wireless sensor network", IET Communication, Vol. 6, Iss. 14, pp. 2149–2158.
[20] K.Akkaya, I. F. Senturk, S.Vemulapalli, 2013, "Handling large-scale node failures in mobile sensor/robot networks", Elsevier Journal of Network and Computer Applications, pp.195-210.

AUTHORS PROFILE

Dr. Deepak Dadwal isB.Tech,M.Tech,Ph.D in Electronics and Communication Engineering. Currently he is working as an associate professor in Department of Electronics and Communication ,CGC landran. He domain of research is optical networks,wireless network.

Prof.(Dr.) Vinay Bhatia is a B.Tech, M.Tech, Ph.D in Electronics and Communication Engineering. Currently he is serving as Professor and Head, Department of Electronics and Communication Engineering at CGC landran. He has authored about 90 research papers in various national/international conferences/journals.Currently he is working on routing and security issues pertaining to wireless networks. His main research interests include mobile and adhoc wireless networks, wireless mesh networks and wireless securities

Dr. P.N. Hrisheekeshais B.Tech, M. Tech. Ph. D. from IIT Roorkee. He got more than 28 years' experience in academics, industry and administration, more than 8 years in research and development. He has got more than 50 publications in reputed international and national journal and conference, research consultant for few industries. Has completed so may funded projects. He is the editor of few reputed journals. Guided more than 50 PG and few Ph.D.has few patents and books to his credit. Has established many incubation center ,center of innovation, new leptophos area of research and interest ,renewableenergysources,powersystem,distributionsystem,automation,imageprocessing,energy,audit printing electronics,, AI, ,machine learning etc.

Retrieval Number: I11260789S19/19©BEIESP
DOI: 10.35940/ijitee.I1126.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication