COMPARITIVE PERFORMANCE ANALYSIS OF ZRP AND DSDV ROUTING PROTOCOL AND IDENTIFICATION OF MALICIOUS NODE IN A CLUSTERED HETEROGENEOUS WIRELESS SENSOR NETWORK

Priyanka D.L[1], Prashanth C R[2] Lakshmi M [3]

[1] M.Tech Student, Dept of Telecommunication Engineering

[2] Professor, Dept of Telecommunication Engineering

[3] Research Scholar Dept of Telecommunication Engineering

[1, 2,3]Dr. Ambedkar Institute of Technology, Bengaluru

Abstract: *The present work focuses on the study on performance analysis of DSDV and ZRP routing protocols in clustered heterogeneous wireless sensor network. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks. The clustered network mainly defines the nodes with different configuration. The system model includes a base station and several sensor nodes within a sensing area. Nodes are classified into cluster heads and cluster members. Clustering sensors into groups, so that sensors communicate information only to cluster heads and then the cluster heads communicate the aggregated information to the processing centre, saving energy and bandwidth. Identification of malicious node due to routing attacks on clusters by routing protocols. Data Aggregation is a technique which is to reduce the energy cost further by reducing the amount of data in transit. And also performance comparison of protocols such as ZRP and DSDV studied with network parameters.*

Index Terms- **Wireless Sensor Network, NHSEP algorithm, ZRP and DSDV**

I.INTRODUCTION

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. This networks are perfect possibility for observing situations in a wide variety of utilizations for example, military reconnaissance and backwoods fire screen. Remote sensor systems are by and large provisioned to comprise of an extensive number of modest nodes detailing their information to a focal ground-breaking hub utilizing multi jump transmission

Remote sensor organize is the data preparing approach and developing territory of the exploration in this decade.

WSN is the accumulation of minor sensor hubs that conveyed in the sensible system field. Remote sensor arranged give the usefulness of transmitting the information starting with one end then onto the next end in the system and sharing the information among various sensor hubs in the sensor field. Sensor hubs placed with inbuilt detecting, correspondence capacities, information gathering, handling capacity, constrained battery power and restricted storage room too. Versatility is the vitality devouring procedure on the grounds that in this procedure hubs ought to be move in the detecting field according to portability display utilized like gathering based, passerby or arbitrary way point portability demonstrate. Some time versatility demonstrate give time viable arrangement.

II. RELATED WORK

Shahjahan Ali and Parma Nand [1] proposed a framework which demonstrates the execution investigation of AODV and DSR directing convention under wormhole assault in MANET by changing the hub speed. Different security assaults can influence the throughput, end-to-end delay, bundle conveyance proportion of AODV and DSR directing conventions. Wormhole is such sort of assault. They proposed the near execution investigation of AODV and DSR directing conventions under wormhole assault in Mobile Ad-Hock arrange is done.

Manoj Kumar and Sujata Negi Thakur [2] recommended that Comparative investigation and execution examination of different specially appointed steering conventions. They exhibited relative examination of existing steering conventions like Ad Hoc on Demand Multipath. Distance Vector (AOMDV), Destination-Sequenced Distance-Vector Routing (DSDV) and Zone Routing Protocol (ZRP). Reenactment comes about demonstrate that AOMDV performs superior to DSDV and ZRP convention by over 14% and 59% individually in bundle conveyance proportion and AOMDV, DSDV both perform superior to ZRP regarding Throughput and normal End-To-End Delay.

Rajendra Singh Bisht [3] suggested that progressive system has the better execution when contrast and that of non-various leveled directing method. Various leveled trip conventions are basic for the remote sensor systems (WSN) to amplify its lifetime. Vitality utilization and system life time has been considered as the real issues.

Sake Purpose Pothalaiah,et al., [4] recommended that New Hierarchical Stable Election Protocol (NHSEP) clustering is done symmetrically and the best hub as for remained vitality and separation of different hubs in contrasting and every that chose as a group head. In this paper execution of the LEACH, SEP and NHSEP conventions need to assess and recreation comes about were do utilizing NS2 test system and contrast and parameters Energy Consumed, Energy Remaining, Packet Delivery Fraction as well as End to End Delay

Vishnu Pratap Singh Kirar et al., [5] have proposed a study of assaults and security necessities in remote sensor systems and also proposed about security necessity of WSN must incorporate properties, for example, classification, uprightness, information freshness, accessibility, and verification. All system models permit arrangements for executing above said properties keeping in mind the end goal to guarantee assurance against assaults to which these kinds of systems are powerless. Assaults can happen at any layer, for example, physical, connect, system, transport, and application and so forth.

Manish M Patel and Akshai Aggarwal [6] proposed that suggested that Wireless Sensor Network is being developed as an overall innovation in future because of its extensive variety of utilizations in military and regular citizen areas. There are part of assaults on these systems which can be named directing assaults and information activity assaults. A portion of the information assaults in sensor hubs are wormhole.

Rupinder Singh et al.,[7] have proposed gathering of spatially scattered and devoted sensors for observing and recording the physical states of nature and sorting out the gathered information at a focal area. WSNs measure natural conditions like temperature, sound, contamination levels, moistness, wind speed and heading, weight, and so forth. The sensor hubs have extraordinary asset restrictions, temperamental correspondence medium and that too in unattended conditions. This makes it extremely troublesome for the usage of the current security ways to deal with WSNs because of the multifaceted nature of the current calculations. In this paper we initially examine different issues and necessities worry with the security of WSNs and after that we talk about in insight about layer astute assaults in WSNs. A detail investigation of these assaults will help in the plan of powerful and proficient countermeasures for assaults against WSNs.

Mukesh Tiwari et al.,[8] have the remote sensor systems (WSNs) are being sent every now and again in assortment of situations. Sensor hubs have constrained correspondence ability and low calculation assets so every hub is frail element that can be effortlessly imperiled by foe by propelling malevolent programming inside the system .Performance assessment of remote sensor organize requires reasonable displaying of Intrusion location framework since the majority of WSNs are application particular. They paper presents a detail based Intrusion Detection System for remote sensor systems.

Kiran Maraiya, et al., [9] have proposed the system life time can be improved with the approach of Data collection. Information accumulation is exceptionally essential strategies in remote sensor arrange. Since with the assistance of information collection we diminish the vitality utilization by taking out repetition..In this paper we talk about the information total methodologies in light of the steering conventions, the calculation in the remote sensor organize. And furthermore examined the points of interest and disservices or different execution measures of the information collection in the network.

Aykut Karakaya and Sedat Akleylek [10] have proposed information acquired from the sensors must be transmitted securely to the objective. Remote sensor systems have an expansive number of assault writes (Sybil, Wormhole, Sinkhole, and so forth.) that debilitate information stream. While planning security strategies, a general structure is gone for wiping out a few or the majority of the assaults. Hence, strategies in light of data security standards, for example, protection, trustworthiness, accessibility, verification and nonrepudiation have been produced. In this paper, current issues are surveyed in the security of remote sensor systems, and validation security approaches are talked about.

Roshan Jahan [11] ,have proposed the detection of malicious node and deployment of routing strategy in Wireless Sensor Networks and also proposed routing in vehicular ad-hoc network is current area of research due to fast mobility of vehicles. A new route in very less time has to be developed

to communicate with the base station. If any node behaving like malicious and creates attack on network, than whole communication will be squeeze. They presents a routing strategy to prevent from attack and identify the malicious node. The strategy has been implemented on and compared with other routing protocols in the presence of malicious nodes.

B. K. Mishra,, et al., [12] presented that a remote sensor organize comprises of topographically appropriated self-sufficient sensors to screen and control over physical or natural conditions. Close-by numerous methods have been proposed in the writing for identification and counteractive action of dark gap assault in sensor organize. There are different arrangements proposed in the writing which recognizes dark opening assault and gives effective conveyance of information to the base station.

Mousam Dagar and Shilpa Mahajan [13] proposed that wireless sensor network comprise of sensor hubs. These systems have tremendous application in natural surroundings checking, fiasco administration, security and military, and so on. Remote sensor hubs are little in measure and have constrained handling ability low battery control.. In this paper it is mainly about information accumulation and its different vitality productive system utilized for information collection in WSN.

Sukhwinder Singh , et al., [14] proposed that improvement of convention by scaling it to numerous levels to increase vitality effective information total. The paper shows a procedure called as Mobility-empowered Multi Level Optimization (MeMLO) that tending to the current issue of bunching in remote sensor net-work (WSN).The recreation result demonstrates insignificant computational com-plexity, quicker reaction time, and exceedingly vitality effective for expansive scale WSN for longer reproduction adjusts when contrasted with traditional LEACH calculation.

Radhika Saini and Manju Khari [15] have presented that any hub in specially appointed system displays an atypical conduct called the noxious conduct. In this circumstance, the whole task of a system gets irritated and to block such vindictive conduct a few security arrangements have been found. In this paper, noxious conduct of a hub is characterized and to guard such conduct, security arrangements are exhibited which are utilized as a part of outfitting a safe and dependable correspondence in impromptu.

Shahjahan Ali and Parma Nand [1] proposed a framework which demonstrates the execution investigation of AODV and DSR directing convention under wormhole assault in MANET by changing the hub speed. Different security assaults can influence the throughput, end-to-end delay, bundle conveyance proportion of AODV and DSR directing conventions. Wormhole is such sort of assault. They proposed the near execution investigation of AODV and DSR directing conventions under wormhole assault in Mobile Ad-Hock arrange is done.

Manoj Kumar and Sujata Negi Thakur [2] recommended that Comparative investigation and execution examination of different specially appointed steering conventions. They exhibited relative examination of existing steering conventions like Ad Hoc on Demand Multipath. Distance Vector (AOMDV), Destination-Sequenced Distance-Vector Routing (DSDV) and Zone Routing Protocol (ZRP). Reenactment comes about demonstrate that AOMDV performs superior to DSDV and ZRP convention by over 14% and 59% individually in bundle conveyance proportion and AOMDV, DSDV both perform superior to ZRP regarding Throughput and normal End-To-End Delay.

Rajendra Singh Bisht [3] suggested that progressive system has the better execution when contrast and that of non-various leveled directing method. Various leveled trip conventions are basic for the remote sensor systems (WSN) to amplify its lifetime. Vitality utilization and system life time has been considered as the real issues.

Sake Purpose Pothalaiah,et al., [4] recommended that New Hierarchical Stable Election Protocol (NHSEP) clustering is done symmetrically and the best hub as for remained vitality and separation of different hubs in contrasting and every that chose as a group head. In this paper execution of the LEACH, SEP and NHSEP conventions need to assess and recreation comes about were do utilizing NS2 test system and contrast and parameters Energy Consumed, Energy Remaining, Packet Delivery Fraction as well as End to End Delay

Vishnu Pratap Singh Kirar et al., [5] have proposed a study of assaults and security necessities in remote sensor systems and also proposed about security necessity of WSN must incorporate properties, for example, classification, uprightness, information freshness, accessibility, and verification. All system models permit arrangements for executing above said properties keeping in mind the end goal to guarantee assurance against assaults to which these kinds of systems are powerless. Assaults can happen at any layer, for example, physical, connect, system, transport, and application and so forth.

Manish M Patel and Akshai Aggarwal [6] proposed that suggested that Wireless Sensor Network is being developed as an overall innovation in future because of its extensive variety of utilizations in military and regular citizen areas. There are part of assaults on these systems which can be named directing assaults and information activity assaults. A portion of the information assaults in sensor hubs are wormhole.

Rupinder Singh et al.,[7] have proposed gathering of spatially scattered and devoted sensors for observing and recording the physical states of nature and sorting out the gathered information at a focal area. WSNs measure natural conditions like temperature, sound, contamination levels, moistness, wind speed and heading, weight, and so forth. The sensor hubs have extraordinary asset restrictions, temperamental correspondence medium and that too in unattended conditions. This makes it extremely troublesome for the usage of the current security ways to deal with WSNs because of the multifaceted nature of the current calculations. In this paper we initially examine different issues and necessities worry with the security of WSNs and after that we talk about in insight about layer astute assaults in WSNs. A detail investigation of these assaults will help in the plan of powerful and proficient countermeasures for assaults against WSNs.

Mukesh Tiwari et al.,[8] have the remote sensor systems (WSNs) are being sent every now and again in assortment of situations. Sensor hubs have constrained correspondence ability and low calculation assets so every hub is frail element that can be effortlessly imperiled by foe by propelling malevolent programming inside the system .Performance assessment of remote sensor organize requires reasonable displaying of Intrusion location framework since the majority of WSNs are application particular. They paper presents a detail based Intrusion Detection System for remote sensor systems.

Kiran Maraiya, et al., [9] have proposed the system life time can be improved with the approach of Data collection. Information accumulation is exceptionally essential strategies in remote sensor arrange. Since with the assistance of information collection we diminish the vitality utilization by taking out repetition..In this paper we talk about the information total methodologies in light of the steering conventions, the calculation in the remote sensor organize. And furthermore examined the points of interest and disservices or different execution measures of the information collection in the network.

Aykut Karakaya and Sedat Akleylek [10] have proposed information acquired from the sensors must be transmitted securely to the objective. Remote sensor systems have an expansive number of assault writes (Sybil, Wormhole, Sinkhole, and so forth.) that debilitate information stream. While planning security strategies, a general structure is gone for wiping out a few or the majority of the assaults. Hence, strategies in light of data security standards, for example, protection, trustworthiness, accessibility, verification and nonrepudiation have been produced. In this paper, current issues are surveyed in the security of remote sensor systems, and validation security approaches are talked about.

Roshan Jahan [11] ,have proposed the detection of malicious node and deployment of routing strategy in Wireless Sensor Networks and also proposed routing in vehicular ad-hoc network is current area of research due to fast mobility of vehicles. A new route in very less time has to be developed to communicate with the base station. If any node behaving like malicious and creates attack on network, than whole communication will be squeeze. They presents a routing strategy to prevent from attack and identify the malicious node. The strategy has been implemented on and compared with other routing protocols in the presence of malicious nodes.

B. K. Mishra,, et al., [12] presented that a remote sensor organize comprises of topographically appropriated self-sufficient sensors to screen and control over physical or natural conditions. Close-by numerous methods have been proposed in the writing for identification and counteractive action of dark gap assault in sensor organize. There are different arrangements proposed in the writing which recognizes dark opening assault and gives effective conveyance of information to the base station.

Mousam Dagar and Shilpa Mahajan [13] proposed that wireless sensor network comprise of sensor hubs. These systems have tremendous application in natural surroundings checking, fiasco administration, security and military, and so on. Remote sensor hubs are little in measure and have constrained handling ability low battery control.. In this paper it is mainly about information accumulation and its different vitality productive system utilized for information collection in WSN.

Sukhwinder Singh , et al., [14] proposed that improvement of convention by scaling it to numerous levels to increase vitality effective information total. The paper shows a procedure called as Mobility-empowered Multi Level Optimization (MeMLO) that tending to the current issue of bunching in remote sensor net-work (WSN).The recreation result demonstrates insignificant computational com-plexity, quicker reaction time, and exceedingly vitality effective for expansive scale WSN for longer reproduction adjusts when contrasted with traditional LEACH calculation.

Radhika Saini and Manju Khari [15] have presented that any hub in specially appointed system displays an atypical conduct called the noxious conduct. In this circumstance, the whole task of a system gets irritated and to block such vindictive conduct a few security arrangements have been found. In this paper, noxious conduct of a hub is characterized and to guard such conduct, security arrangements are exhibited which are utilized as a part of outfitting a safe and dependable correspondence in impromptu.

III. METHODOLOGY IN PROPOSED WORK

A. DESIGN GOALS

1) The steps included in the flow diagram of figure 1, initially considered in construction of heterogeneous wireless sensor network .
2) The random deployment of nodes with different configurations is done based on the requirement.
3) With respect to the sequence order, clustering is done using NHSEP. Among the nodes based on the higher energy node is made as a Cluster Head.
4) Authentication of Clusters and finding the malicious node among the clusters.
5) Recovering of the node in each clusters being attacked from different attacks.
6) Data aggregation is carried out in each clusters
7) Aggregated data is transmitted to the sink
8) Performance comparison of two protocols using network parameters is carried out in order to find the best performed protocol.
9) Second part is followed by primary flow chart, so that basic implementation has done that is shown in figure 2.
10) Third part is followed by second flow chart remaing part of implementation is shown in figure 3. These proposed work is challenging task because it is depending on various factors like packet loss, energy efficiency and through put of the system and to give the protection for the primary users.

B. ALGORITHM USED IN PROPSED WORK

1. Problem formulation

Along with the performance analysis of protocols cluster formation, based on higher energy cluster head formation, authentication where mainly on the node having the lower energy is the malicious node thus data loss occurs and recovery of dropped nodes concern with protection avoid the duplication, missing without notice will makes changes in the network paraameters such as packet delivery ratio, bit error rate, throughput, energy as well as control overhead.

2. CLUSTER FORMATION

- First step involves the deployment of nodes with different configuration.
- Initially nodes are configured randomly.
- Next step is to find energy for each node (Hello packet transmission).
- Next is to make clusters among the nodes where each cluster has 20 nodes so finally five clusters are formed with an individual sink. sorting of the energy of each node and choosing highest energy node.

3. HETEROGENEOUS NEW HIERARCHICAL STABLE ELECTION PROTOCOL

1. The base station (BS) is located far from the sensors and immobile.
2. All nodes in the network are heterogeneous
3. and energy constrained.
4. All nodes are able to send data to BS.
5. The BS has the information about the location of each node.
6. sorting of the energy of each node and choosing highest energy node as cluster head.
7. Cluster-heads (CHs) perform data reception and transmission.
8. At the start energy of all nodes is at the maximum level.
9. In the first round, each node has a probability p of becoming the cluster head.
10. A node which has become cluster head shall be eligible to become cluster head after 1/p rounds.
11. Nodes in the network are not dynamic while the Cluster Heads (CHs) are being selected

4. Proposed Work Detailed Design

In NS2 architecture, the generic steps involved in implementation are as follows.

- Set up the required number of nodes and so on. There are 90 nodes created in grid layout form.
- Create the simulator
- Set the trace and logging information.
- Set the Network Animator(NAM) window.

C. PROPOSED MODEL

The following models shown in figure 1, 2 and 3 focuses on the detailing flow of the proposed work .Here figure 1 represents the detailed flow of implementation, figure 2 shows first part of implementation till the node configuration in wireless sensor network and finally figure 3 presents the details from cluster head formation to final data transmission to sink.

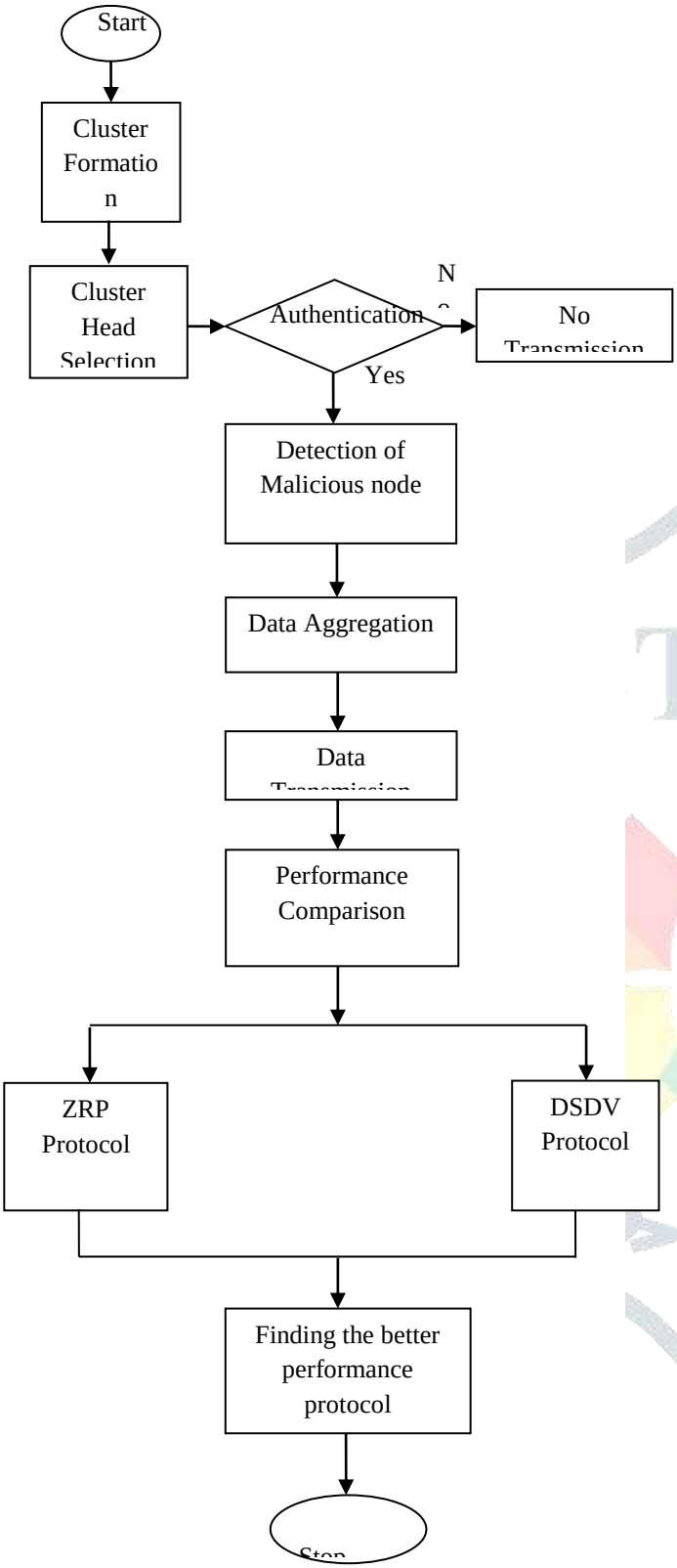

fig 1: flow chart of proposed model

Fig.1: Implementation Flow Chart

(i)FIRST PART OF THE PROPOSED MODEL

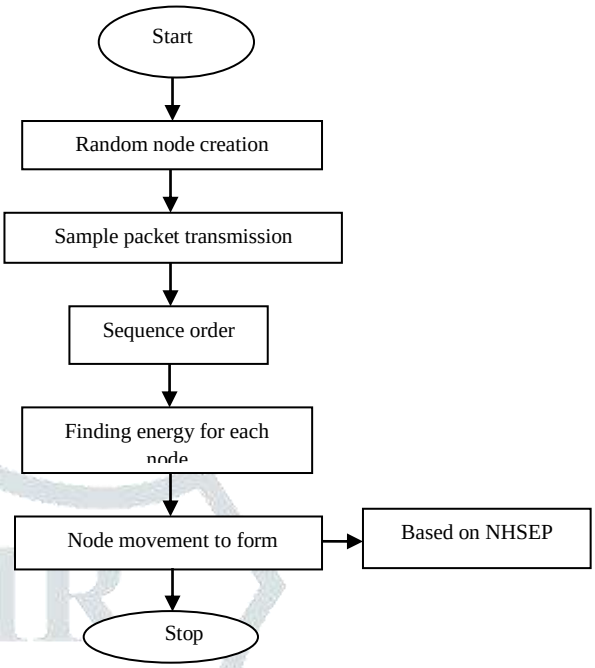

Fig.2: Implementation flow of node configuration

(ii) SECOND PART OF THE PROPOSED SYSTEM

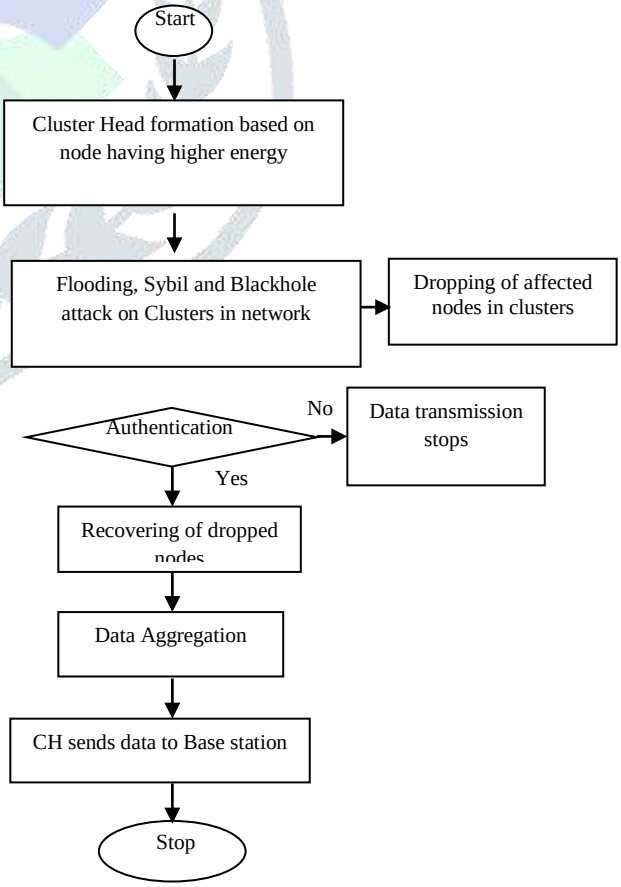

Fig.3: Implementation flow from CH formation to final data transmission to BS

IV. DESIGN OF IMPLEMENTED WORK

The simulation output such as configuration of nodes, cluster formation, cluster head formation, attacks on clusters, authentication, recovery of nodes, data aggregation and performance comparisons of DSDV and ZRP protocols with respect to network parameters such as energy, bit error rate, packet delivery ratio and throughput in Network Animator window.

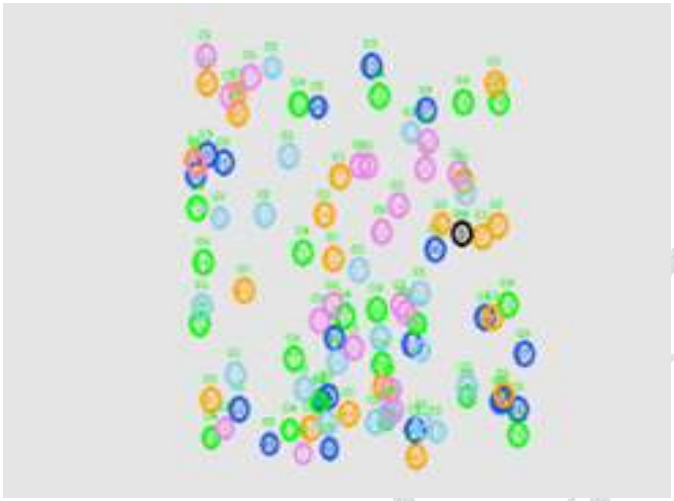

Fig.4: Node configuration

As shown in figure , output has total of 101 nodes that are created. Where 100 nodes are considered as source and one node is considered as sink as shown in multiple colors. As explained in the design, the distance between each and every pair will be calculated. If the distance is less than transmission range i.e then that node will be considered as neighbor (i.e. Cluster Member). The node which has a highest number of probabilities is being considered as a source node or destination node and is shown in red color.

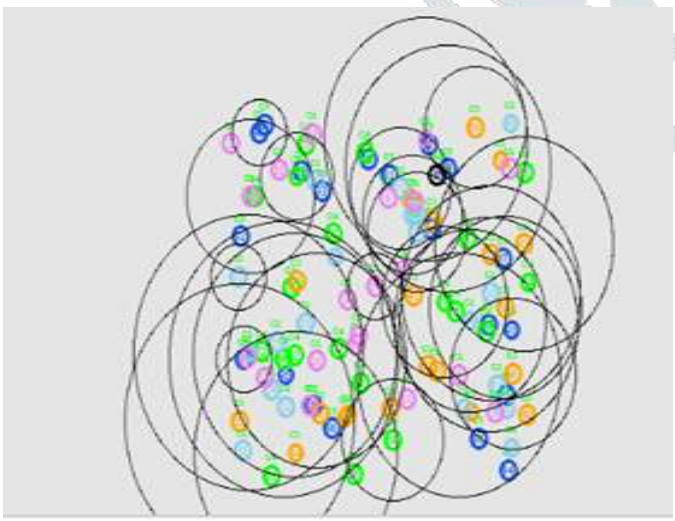

Fig.5: Transmission of sample packets

Transmission of sample packets as shown in the above figure, hello packet transmission has done so that each node gets into active mode from sleep mode so that started sensing over sensing area in the deployed wireless sensor network.

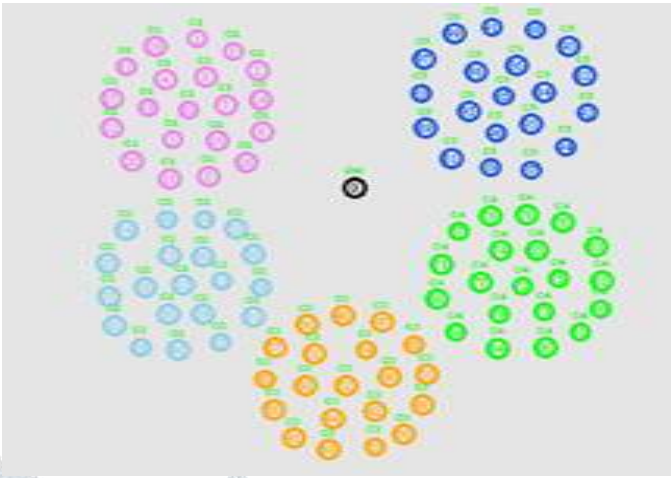

Fig.6: Cluster Formation

The shown in figure nodes are formed into clusters based on sequence order using New Hierarchical Stable Election Protocol (NHSEP) so that five clusters are made each cluster has ten nodes . Theses clusters are source and the remaining node is considered as sink. Their exist a Robustness Load Balancing Scalability and Energy Efficiency in the network.

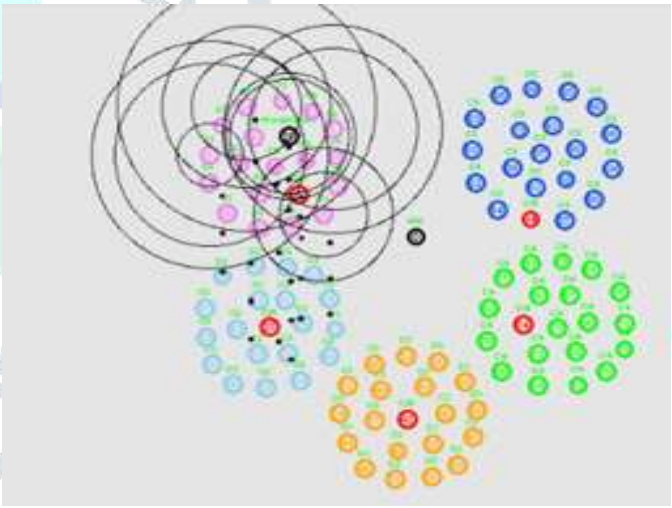

Fig.7: Flooding attack on cluster 1

As shown in the above figure 7 the attacker creates an illusion of being a neighbour to other nodes and underlying routing protocol can be disrupted which facilitate further types of attacks. Here cluster one is attacked by the flooding attack due to this affected nodes are dropped from the cluster one as shown.

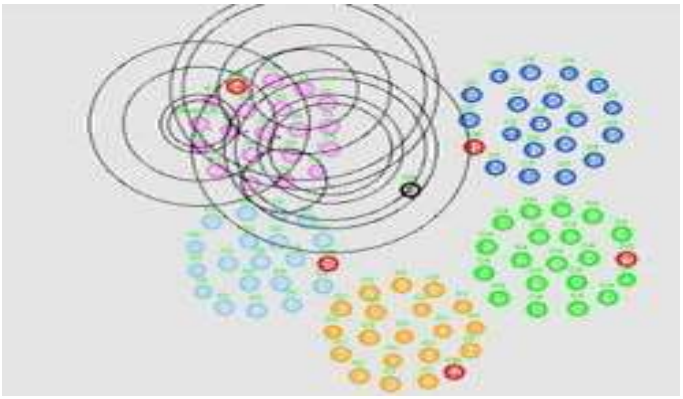

Fig.8: Recovering of affected node in cluster 1

In cluster one nodes were dropped due to flooding attack so that the loss of data along with attacked node has happened. Finally te dropped nodes are recovered back as shown in the figure 8.

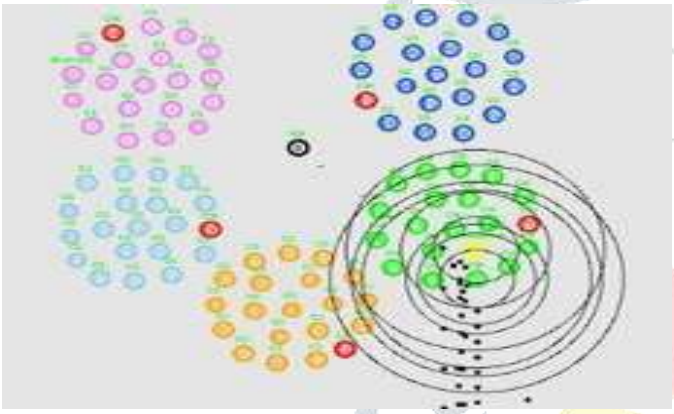

Fig.9: Sybil attack on cluster 4

In this sybil attack mainly malicious nodes used by attackers creates large number of entities so that gained by influence in traffic network. Malicious has particular ID's to make fake addition and duplication among original entities. The Here cluster four is attacked by the sybil attack due to this affected nodes are dropped from the cluster four as shown in figure 9.

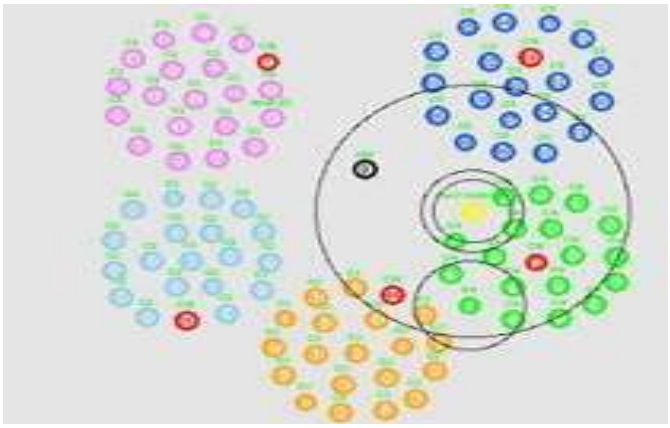

Fig 10: Recovering of affected node in cluster 4

As shown in the figure 10 above in cluster four the nodes were dropped due to sybil attack so that the loss of data along with attacked node has happened. Finally the dropped nodes are recovered back.

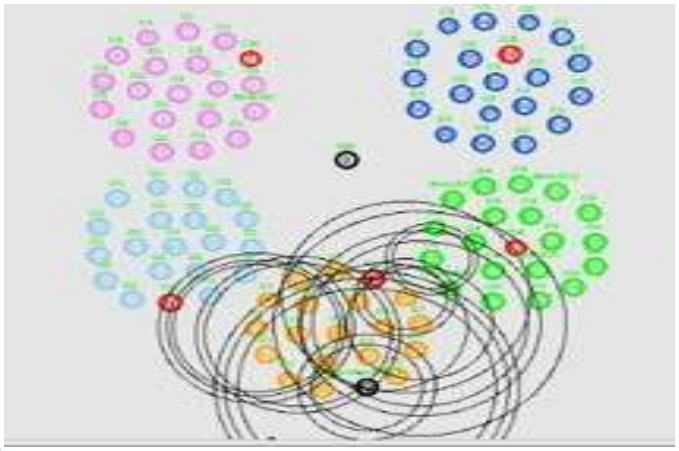

Fig.11: Black hole attack on cluster 3

In this above figure 11 cluster three is attacked by the blackhole attack in which malicious node become more attractive to nodes around that. Due to this affected nodes are dropped from the cluster.

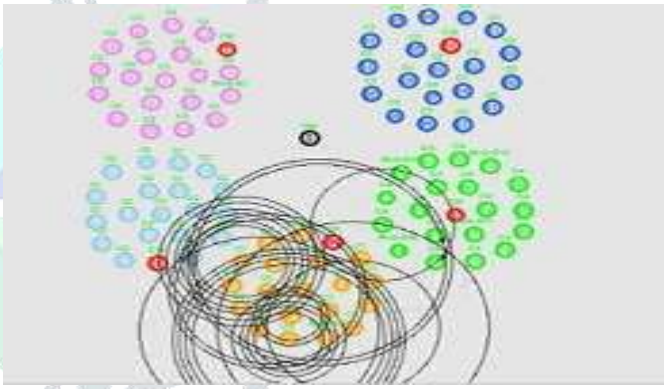

Fig 12: Recovering of affected node in cluster 3

The cluster three nodes were dropped due to flooding attack so that the loss of data along with attacked node has happened. Finally the dropped nodes are recovered back as shown in the figure 12.

Data Aggregation is a technique which is the energy cost further by reducing the amount of data in transit. It is believed that closely spaced sensor nodes sense data that are spatially correlated. Thus redundancy exists in the data, which can be removed by data aggregation. The amount of data transmitted to the access point is thus reduced and the transmission cost is also reduced.

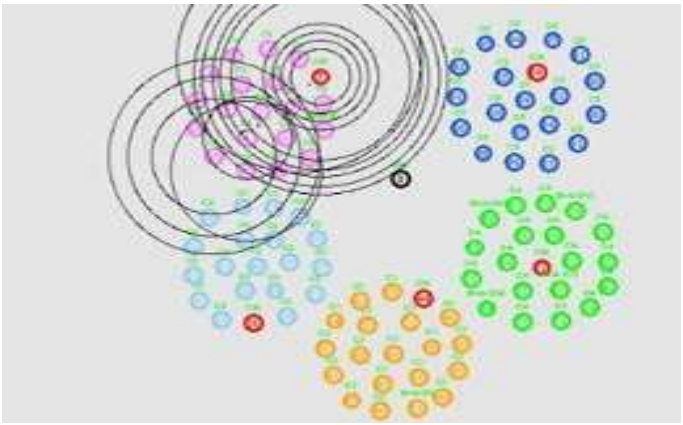

Fig.13 : Data transmission from cluster head to base station

As shown above the most preferred way in saving energy is removing redundancy transmission and collected information to base station. This illustrates that the in cluster one cluster head initially collects all the gathered data and then transmits finally to base station as shown in figure 13.

V. RESULTS AND PERFORMANCE ANALYSIS

A. Graph of Comparative performance analysis of DSDV and ZRP protocols based on network parameters.

As shown in graph, the proposed work with respect to packet to delivery ratio vs node. ZRP has more Packet Delivery Ratio than that of the DSDVwith respect to the node in that of X-axis and packet delivery ratio along Y-axis. So ZRP is more efficient than DSDV.

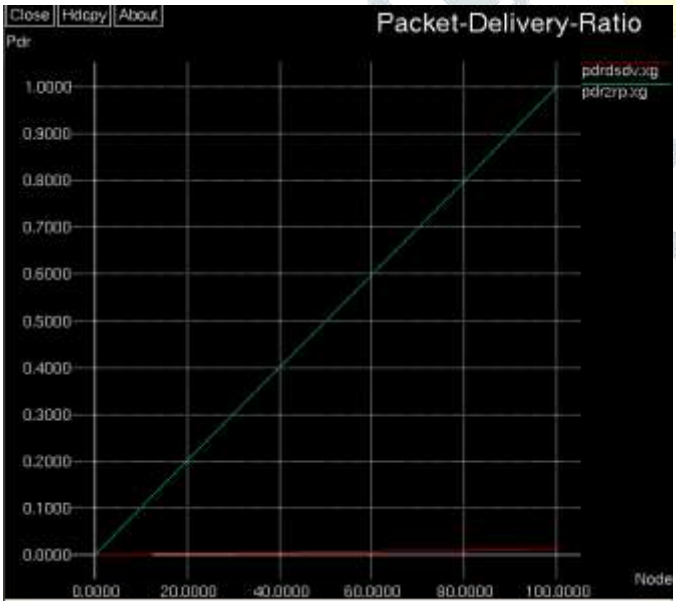

Fig.14 : Packet Delivery Ratio comparision between DSDV and ZRP protocol

As shown in graph, the comparison of proposed work with respect to throughput v/s node from the source to destination communication. ZRP has more Throughput than that of DSDV with respect to the node in X-axis and throughput in Y-axis. As the deployed node number increases the throughput also increases so ZRP is more Efficient.

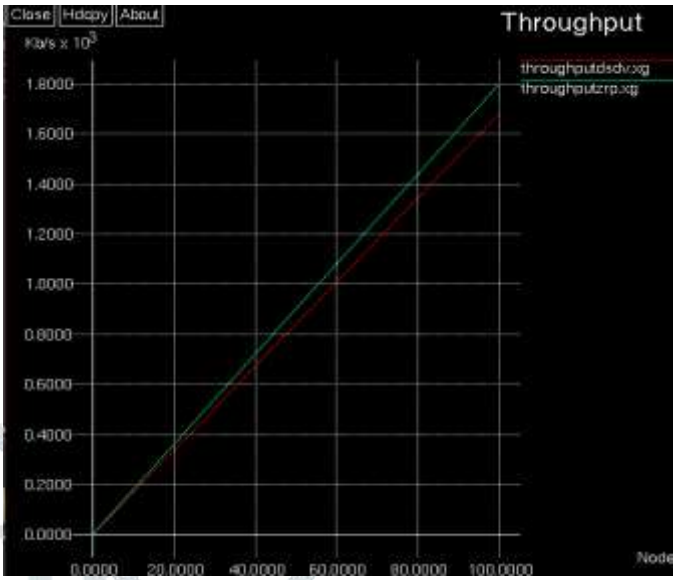

Fig.15: Throughput comparision between DSDV and ZRP protocol.

As shown in graph, the comparison of proposed work with respect to energy v/s node from the source to destination communication. Based on node having the higher energy where it is considered as cluster head among the clusters and this cluster head usually sends the information to base station

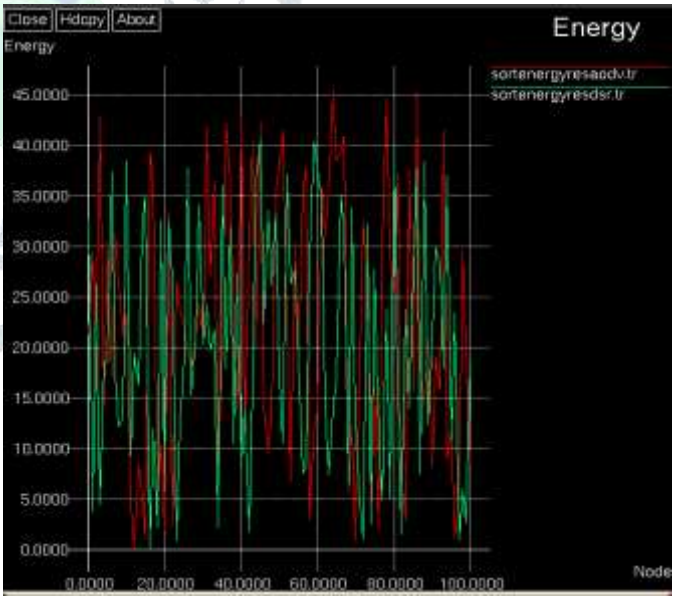

Fig.16 : Energy comparision comparision between DSDV and ZRP protocol

As shown in graph, the packet drop above ZRP has less Bit Error Rate than that of DSDV with respect to the node with respect to X-axis and number of packet loss along Y-axis. Number of packet loss is more in DSDV than ZRP so ZRP is more efficient than DSDV.

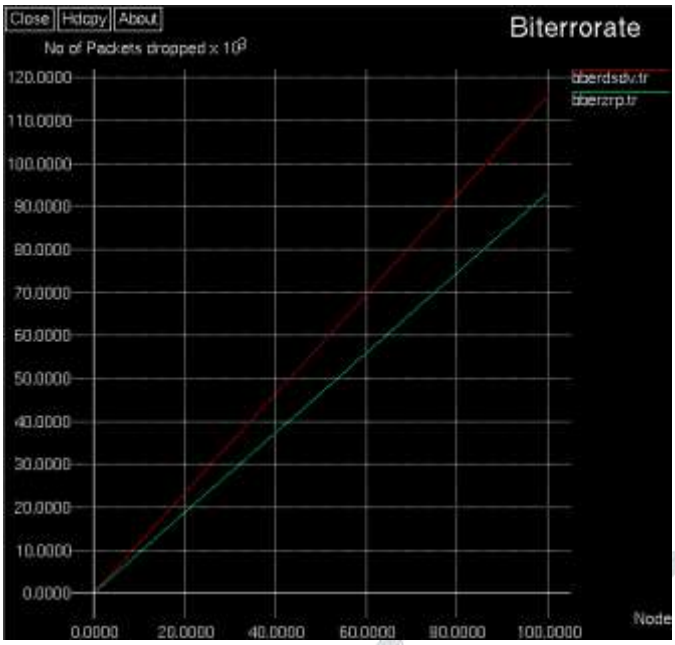

Fig.17 : Bit Error Rate comparision between DSDV and ZRP protocol

B. Performance Analysis

Table 1: Comparative analysis of Network parameters with respect to nodes.

Protocol	Node	Throughput	Energy	Packet Delivery ratio	Bit Error Rate
ZRP	25	450.215	49.3066	0.25	23343.5
	50	900.43	49.3069	0.50	46687
	75	1350.64	49.3077	0.75	70030.5
	100	1800.86	49.3103	1	93374
DSDV	25	420.08	49.3097	0.003	29005.25
	50	840.179	49.3086	0.006	58010.5
	75	1260.26	49.3073	0.010	87015.75
	100	1680.358	49.3092	0.013	116021

As shown in table the parameters such as throughput, bit error rate, packet delivery ratio and energy are compared between ZRP and DSDV routing protocols. With respect to nodes parameters are determined, thus it states ZRP is more efficient than the DSDV protocol in simulation.

VI. CONCLUSION

I In this paper wireless sensor network is considered, where clustered heterogeneous network that is sensor with different configuration is deployed randomly. Each node is having sequence order based on that clusters are formed. In each cluster, node having higher energy is elected as cluster head. This cluster head aggregates the information from each node and finally forwards to base station. Routing attacks on the clusters are identified as well as dropped nodes due to attacks are recovered back. Here routing protocols such as ZRP and DSDV are used to find malicious node due to attacks on cluster. Comparison is done among these two protocols based on the network parameters such as throughput, energy, bit error rate, packet delivery ratio and control overhead. ZRP is more efficient than DSDV based on parameter comparison. The future work is primarily concentrating on the new routing calculation to course the information from source to the sink.The principle challenge is to beat the issues in topology development information directing expense can be diminished by reformation systems.

REFERENCES

[1]Shahjahan Ali and Parma Nand," Comparative Performance Analysis of AODV and DSR Routing Protocols under Wormhole Attack in Mobile Ad Hoc Network on Different Node's Speeds", *IEEE International Conference on Computing, Communication and Automation* 2016.

[2]Manoj Kumar and Sujata Negi Thakur , "Comparison of DSDV, DSR and ZRP Routing Protocols in MANETs", *International Journal of Computer Applications,* Volume 108, December 2014.

[3]Rajendra Singh Bisht, "Performance Analysis Of Hierarchical And Non-Hierarchical Routing Techniques In Wireless Sensor Networks", *IEEE International Conference on Soft Computing Techniques and Implementations* 2015 .

[4]Sake Pothalaiah and D. Sreenivasa Rao, "New Hierarchical Stable Election Protocol for Wireless Sensor Networks", *IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems* 2015.

[5]Vishnu Pratap Singh Kirar, " A Survey of Attacks and Security Requirements in Wireless Sensor Networks", *Engineering and Technology International Journal of Electronics and Communication Engineering* Vol:8, No:12, 2014

[6] Mr. Manish M Patel and Dr. Akshai Aggarwal "Security Attacks in Wireless Sensor Networks: A Survey". *International Conference on Intelligent Systems and Signal Processing (ISSP).* 2013

[7] Rupinder Singh and Jatinder Singh" Attacks In Wireless Sensor Networks: A Survey". *International Journal of Computer Science and Mobile Computing. IJCSMC, Vol. 5, Issue. 5, pg.10 – 16,* May 2016.

[8] Mukesh Tiwari and Karm Veer "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information*".Fourth*

International Conference on Computer Sciences and Convergence Information Technology.2009.

[9] Kiran Maraiya, Kamal Kant, Nitin Gupta" Wireless Sensor Network: A Review on Data Aggregation" *International Journal of Scientific & Engineering Research Volume 2, Issue 4*, April -2011.

[10]" Aykut Karakaya and Sedat Akleylek A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks",IEEE.2018.

[11] Roshan Jahan and Preetam Suman"Detection of malicious node and development of routing strategy in VANET".2016.

[12] B. K. Mishra, M.C. Nikam, P. Lakkadwala, "Security against Black Hole Attack in Wireless Sensor Network - A Review," *Fourth International Conference on Communication Systems and Network Technologies* (CSNT), pp. 615-620, April 2014.

[13] Mousam Dagar and Shilpa Mahajan "Data Aggregation in Wireless Sensor Network: A Survey" *International Journal of Information and Computation Technology*. Volume 3, Number 3, pp. 167-174, 2013.

[14] Sukhwinder Singh Sran and Lakhwinder Kaur "Energy Aware Chain Based Data Aggregation Scheme for Wireless Sensor Network" , *International Conference on Energy Systems and Applications*, 30 Oct - 01 Nov, 2015.

[15] Radhika Saini and Manju Khari "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network". *International Journal of Computer Applications (0975 – 8887) Volume 20– No.4*, April 2011.

BIOGRAPHIES

Priyanka D.L received the B E degree in Telecommunication Engineering from BMS College of Engineering, Bangalore and currently pursuing her Masters in Digital Communication and Networking in Dr. Ambedkar Institute of Technology, Bangalore. Her research interests include Communication Engineering, Wireless Sensor Networks and Digital Communication.

Dr. Prashanth C R received the B E degree in Electronics in Digital Communication and Networking and the Ph.D. degree in Computer Science from Bangalore University, Bangalore. He is currently Professor, Department of Telecommunication Engineering, P G Coordinator, and Deputy Controller of Examinations, Dr. Ambedkar Institute of Technology, Bangalore. His research interests include Image Processing, Pattern Recognition, Biometrics, Computer Networks, Communication Engineering and Nano Physics. He has served as a member of Board of Examiners for Bangalore University and Visvesvaraya Technological University. He is a member of IEEE, ACM and IACSIT, and life member of Indian Society for Technical Education, New Delhi and Fellow of Institution of Engineers (India).

Lakshmi . M received the B E degree in Telecommunication Engineering from R.V College of Engineering, Bangalore, Masters in Masters in Digital Communication and Networking in Dr. Ambedkar Institute of Technology, Bangalore. currently pursuing her Ph.D in Dr. Ambedkar Institute of Technology, Bangalore.Her research interests include Communication Engineering, Wireless Sensor Networks and Digital Communication.