ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Secure, Consistent and Effective Data Acquisition in Wireless Sensor Networks in the Existence of Transfaulty Nodes

Chetan Patil[1], Prof. M. D. Ingle[2], Prof. S. H. Patil [3]

P.G. Student, Department of Computer Engineering, JSPM's JSCOE, Hadapsar, Pune, India[1]

Associate Professor, Department of Computer Engineering, JSPM's JSCOE, Hadapsar, Pune, India[2]

Associate Professor, Department of Computer Engineering, JSPM's JSCOE, Hadapsar, Pune, India[3]

ABSTRACT: The sensors in the WSN sense the nearby, collects the data and transfers the data to the sink node. It has been noticed that the sensor nodes are incapacitated or weakened when visible to persuaded radiations or due to energy problems. This weakening leads to the transient separation of the nodes from the network which effects in the creation of the holes. These holes are self-motivated in nature and can spread and contract dependent upon the features causing the weakening to the sensor nodes. Thus a solution has been available in the base paper where the twin mode i.e. Radio frequency and the Acoustic mode are considered so that the data can be transferred smoothly. However transferring the data from node to sink we added a hash value for security checking. Based on this a paper has been done where some issues are considered so that the performance and security of the system can be improved.

KEYWORDS: Energy hole problem, Sensor deployment, Wireless Sensor Network.

I. INTRODUCTION

1.1 Wireless sensor networks (WSNs)

The sensor network contains small and a smaller amount of cost sensing devices composed through wireless radio transceiver for inspecting the situation. It contains the data gathering and transferring the information to single or additional sink nodes. The key benefit of this network is that it does not need several arrangement or external source for data gathering [14].

The nodes in the wireless sensor networks contain sensor nodes, sink gateway nodes and the management nodes. Nodes having the capability of composting networks over self-organization are positioned in huge numbers inside or near the observing area. Many nodes handle the observed data, and over multi-hop routing it is transferred to the sink gateway node [15].

The key uses of WSN are remote territory observing, jungle fire recognition, building protection checking, and soldierly stakeout and so on.

The features of WSN, which have caused in interesting topics, are as follows:

- Sensor nodes are unprotected to extreme failures.
- Sensor nodes consume the transmission message configuration and own severe bandwidth limitation.
- Sensor nodes hold rare number of resources.

Due to the inadequate accessibility of resources, the quantity of data broadcast wants to be reduced. This in chance will improve the network lifespan and bandwidth consumption [14].

This can be accomplished through data aggregation.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

1.2 Data aggregation

Data aggregation increases the lifespan of nodes by excluding out of work data broadcast. The data broadcast tracks a multi-hop manner in which every node headlong data to the neighbour node closer to sink. The present methods need be exchanged with an enhanced method by aggregation. Clustering is used where every node directs data to the cluster-head and the received raw data endures aggregation which is then directed to the sink. These aggregation tasks encompass lot of energy wastages. In instance of homogeneous sensor network, the cluster-head will shortly decease and over again re-clustering has to be done which over roots extra energy eating [15].

In contrast, the cluster-head or the aggregator node might be condemned by a mischievous invader. The precision of the aggregated data guided to the base station cannot be sure when the cluster-head is conceded. The uncompromised nodes show some duplicates of aggregated outcome to the base station because of which the power consumed at the nodes is augmented [15].

1.3 Security Requirements

As for as main motive of security services in WSNs is to precaution for the in system and resources from attacks and misbehaviour. The security necessities in WSNs include:

1.3.1 Data Confidentiality:

Data Confidentiality is moreover famous as secrecy of data. As nodes are occasionally used to achieve complex information, it is also a set of procedures that have the restrictions to access the data. Confidentiality is intended to avoid data from attainment the immoral or illegal sensor node. The data should not fall into unintentional hands [16].

1.3.2 Data Integrity:

The method, which guarantees that the broadcast of data from the source to the destination is not ruined, is said to be data integrity. This expose that the data are received deprived of any repetition, addition, and alteration [14].

1.3.3 Data Authentication:

Authentication guarantees the consistency of the message by recognizing its source [14]. Authorization assurances the steady feature of the message by unique its root. Attacks in WSNs don't just contain the packages' alteration; opponents can similarly pervade additional wrong parcels [16].

1.3.4 Data Freshness:

Irrespective of the opportunity that ordering and data decency are definite, there is a necessity to assurance the cleanness of each message. Informally, information cleanness endorses that the information is advanced, and it assurances that no old messages have been repeated [16].

1.3.5 Robustness:

Wireless sensor networks are extremely active and indefinite, as well as modifications in the network topology and the nodes' vanishing or linking. So, the wireless sensor networks in a variation of security assaults must have robust flexibility, and even if a specific attack succeeds, the performance can make the effect reduced [16].

1.3.6 Data Availability:

Data availability stands for the network services want to be accessible uniform through the inside and outside attacks viz. denial of service (DoS) attack. The method that contains in posing accessibility makes use of additional communication services between the nodes or central access control system to guarantee effective transfer of each message to its receiver [16].

1.3.7 Access Control:

Access control needs the capability to recognize the handlers who access wireless sensor networks to guarantee the acceptability. Access control controls who can access the system, what system resources can be gain access to, and how to practice these resources [16].

1.3.8 Non Repudiation:

Non repudiation means if a node direct a message then that node over again send the similar message i.e. that is previously sent [16].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

1.3.9 Forward Secrecy:

Uncertainty any sensor has detached from the network then that node ought to not be capable to deliver the message [16].

1.3.10Backward Secrecy:

A linking sensor should not to have the ability to examine any earlier conveyed message. The security supervisions in WSNs are usually grounded on cryptography. Because of the boundaries in WSNs, several formally present secure designs are not practical for usage.

II. RELATED WORK

The paper offered by the Pushpendu Kar and Sudip Misra Jan 2016 delivers us through the facts of in what way the double mode i.e. radio frequency and the acoustic mode can be applied for the effective and proficient data transfer. Similarly put emphasis on on the data mining process. Due to the suggested system the data can be lead extra proficiently [1].

In the paper offered by Kealan McCusker, Noel E. O'Connor May/June 2011 a solution for allocating symmetric keys and network access control in a WSN using IBC is offered. The suggested system was estimated beside famous attacks on a WSN and found to execute fine. Some groups implement for Tate pairing in hardware but are aiming the latency metric and also Field Programmable Gate Arrays (FPGAs) somewhat than energy and an ASIC, consequently these helps absence above the proposed theory which is numerous scales higher than what is accomplished by applying the coupling in hardware, and too extraordinary for the inadequate energy accessible to a node. Work is required in order to implement additional constituents of the system such as the elliptic curve point multiplication and exponentiation in the field [2].

Cesare Alippi, Giuseppe Anastasi, Mario Di Francesco, and Manuel Roveri Feb 2011. In this paper authors planned an adaptive sampling algorithm that guesses online the ideal sampling frequencies for sensors. This method, which needs the scheme of adaptive measurement systems, reduces the energy eating of the sensors and, incidentally, that of the radio though preserving a very great precision of gathered data. It can accomplish parallel to a fixed-rate system where the sampling frequency is well-known in advance. This method outcomes in a matching energy saving of together the sensor and the radio. Decision intensely rest on the exact sensor, whose power eating is knowingly superior than that of the radio [3].

Levente Buttya´ n, La´ szlo´ Czap, and Istva´n Vajda Nov/Dec 2011. In a pollution attack, the adversary unkindly changes certain of the stored encrypted packets, which outcomes in the improper decrypting of a huge portion of the unique data upon recovery. Authors suggested algorithms to identify and recuperate commencing such attacks. This paper can be functional in any coding-based distributed storage systems, be it in the domain of P2P file distribution or in wireless sensor networks. In particular, this method does not need the storage nodes to accomplish extra coding on or to enhance extra information to the encrypted packets. Suggested algorithm is effective and tremendously proficient together in terms of communication and computational overhead. It does not scale up to very huge schemes in relationships of computational complexity [4].

Ing-Ray Chen, Anh Phan Speer, and Mohamed Eltoweissy March/April 2011. Authors established adaptive fault-tolerant quality of service (QoS) control algorithms grounded on hop-by-hop data transfer using "source" and "path" redundancy, with the objective to fulfill solicitation QoS necessities while extending the lifespan of the sensor system. Algorithm which integrates route and source redundancy mechanisms to fulfill query QoS necessities however maximizing the lifespan of query-based sensor networks. Future work: deliver extra comprehensive study of the outcome of network dynamics on MTTF, such as extra energy may be consumed by some SNs over others or certain SNs may fail prior than others [5].

Masanori Miyazawa and Michiaki Hayashi Rolf Stadler2nd Jan, 2015. The paper suggests a distributed management function, called virtualized network management function(vNMF), to identify disasters associated to virtualized services. vNMF identifies the disasters by monitoring physical-layer statistics that are handled with a self-organizing map algorithm. Memory leaks and network congestion disasters can be effectively noticed and that the correctness of disaster finding can be knowingly enhanced associated to mutual k-means clustering. The suggested vNMF is likely to assist scalable network management in the direction of extra difficult network virtualization environments in the future work [6].

Steven S. McClure, L. D. Edmonds, R. Mihailovich, A. H. Johnston, P. Alonzo, J. DeNatale, Member, IEEE, J. Lehman, and C. Yui Dec 2002. A mechanism for dielectric charge trapping and its consequence on the electrostatic force is suggested. Of prominent consequence is the vulnerability of GaAS MEMS devices to radiation effects, as found in this work. Such properties, if existing, may be removed by appropriate strategy methods, for example demonstrated in the substitute RSC switch configuration. It is powerfully suggested that devices of this type be carefully considered for radiation effects earlier to consumption in systems with a space or nuclear radiation environments. [7].

Erfan Soltanmohammadi, Mahdi Orooji, Mort Naraghi-Pour Jan 2013. The problem of decentralized recognition in wireless sensor networks in the existence of one or extra classes of mischievous nodes. Binary proposition testing is deliberated where the truthful nodes convey their binary choices to the fusion center (FC), while the mischievous nodes convey false messages the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

problematic of decentralized detection in wireless sensor networks in the presence of one or more classes of mischievous nodes. Binary proposition testing is considered where the truthful nodes convey their binary decisions to the fusion center (FC), while the mischievous nodes convey false messages [8].

Tapas Kanungo, David M. Mount, Nathan S. Netanyahu, Christine D. Piatko, Ruth Silverman, and Angela Y. Wu July 2002 Suggested in 2 ways: First, authors contemporary a data-sensitive examination of the algorithm's running time, which illustrate that the algorithm runs quicker as the parting between clusters rises. Second, a number of practical studies both on synthetically produced data and on real data sets as of applications in colour quantization, data compression, and image segmentation. A modest and proficient execution of Lloyd's k-means clustering algorithm, which we call the filtering algorithm. The benefit of this algorithm is it needs a kd-tree as the single major data structure. This algorithm is fairly difficult and does not deliver considerably faster running time in exercise [9].

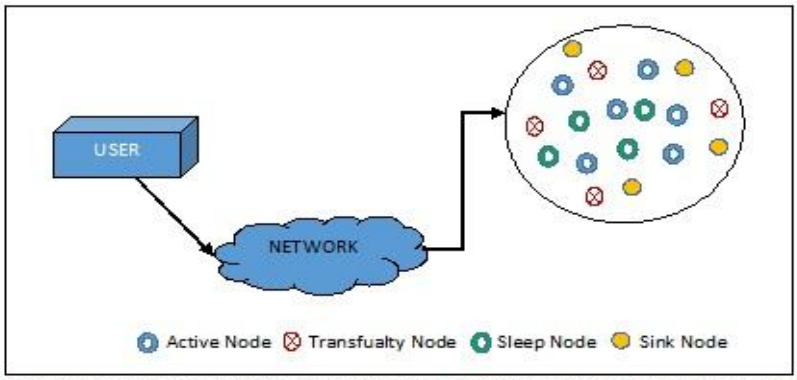
Vibha Paradkar, Gajendra Singh Chandel, Kailash Patidar,2015 suggests a fresh routing algorithm (Master/Slave) for detection and retrieval of the routing path proficiently. The main path, subordinate path and the segmentation process supports to traverse the data from the non-faulty nodes [10]. Also multipath routing supports transfer data all together thus by decreasing delay and congestion in the network [12].

Saad Ahmad Khan, Ladislau Bölöni, Damla Turgut, 2015 the paper suggests a model where the bridge nodes are secure by giving certain accountabilities of the sink nodes to the other nodes. It avoids the apparition of the extra link nodes. The drawback is that the algorithm costs the length of certain routes in order to allocate the routes away from the critical area [11].

Amit Sharma, Kshitij Shinghal, Neelam Srivastava, Raghuvir Singh, Mar 2011 in this work study of the energy eating of a WSN node is studied with proposed node. With the help of this the projected lifespan of the battery can be improved expressively [14]. It is pragmatic that sensors are recycled for promoting data to sink straight so as to decrease energy eating, packet loss and delay [13].

III. WORK OF PROPOSED SYSTEM

The architecture diagram of the system shown below helps us to understand the system.



Architecture Of Consistent and Effective Data Acquisition in WSN in the Existence of Transfaulty Nodes

Fig 1:- System Architecture

We have arranged GPS permitted homogeneous sensor nodes to build a WSN. Here all of the sensor nodes have the identical ability of sensing, transmitting, and receiving. All node identify their position by GPS or any location services. To work in radiation-prone environments and carry on communication between sensor nodes, a node has double mode of communication. The double mode consist of radio frequency (RF) communication mode and acoustic communication mode. Typically a sensor node transfers via the RF communication mode. The RF communication come to be exaggerated due to the effects of radiations, which inactivates the sensor nodes from communicating. Hence, in the existence of radiation effects, the sensor nodes change to the acoustic communication mode. Acoustic communication does not get exaggerated by radiations. Therefore, the sensor nodes remain their communication in the existence of radiations via the acoustic communication mode.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

IV. ALGORITHM

Algorithm 1 Pseudo code of propose system is,

Input V= Set of all nodes

1. Initialize Active Node Sleep Node (AN SN)
2. Broadcast Hello Message
3. Create NetInfo Table
4. Compare NetInfo Table with current neighbor list If list mismatch declare node as Transfaulty Node.
5. Identify boundary Node
6. Activate dual mode of communication
7. Generate Hash Value for sensed data
8. At Sink Check for hash value
9. If hash value is same accept data
10. Else Reject Data
11. Forward Data to Base Station.

V. ANALYSIS AND RESULT

Security Comparison Graph

Figure 2 shows security comparison between existing system & proposed system. We achieved more security in proposed system is more than the existing system.

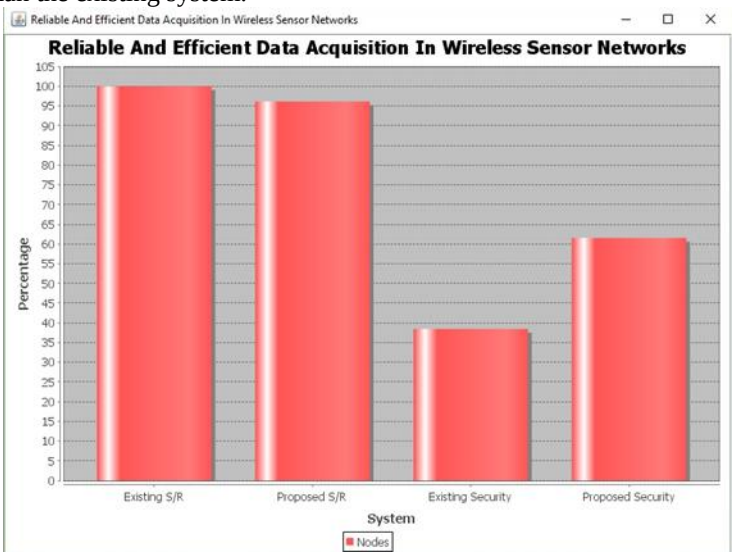


Fig 2. Security Comparison between Existing System & Proposed System.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Energy Graph

Figure 3 shows energy comparison between existing system & proposed system. In existing system there is more energy required. We achieved less energy in proposed system is more than the existing system. Also shown the difference between them.

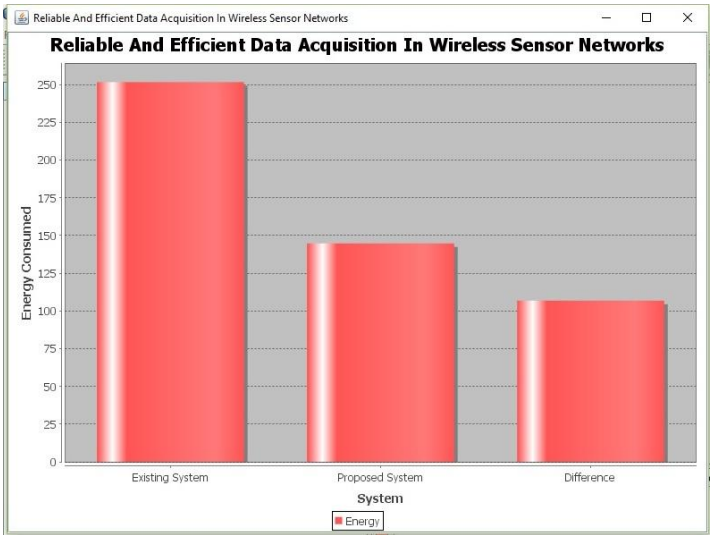


Fig 3. Energy Consumption between Existing System & Proposed System.

Time Delay Graph

Figure 4 shows time delay comparison between existing system & proposed system. In existing system it takes more time to delivered data from source to destination. We achieved less time delay in proposed system is more than the existing system. Also shown the difference between them.

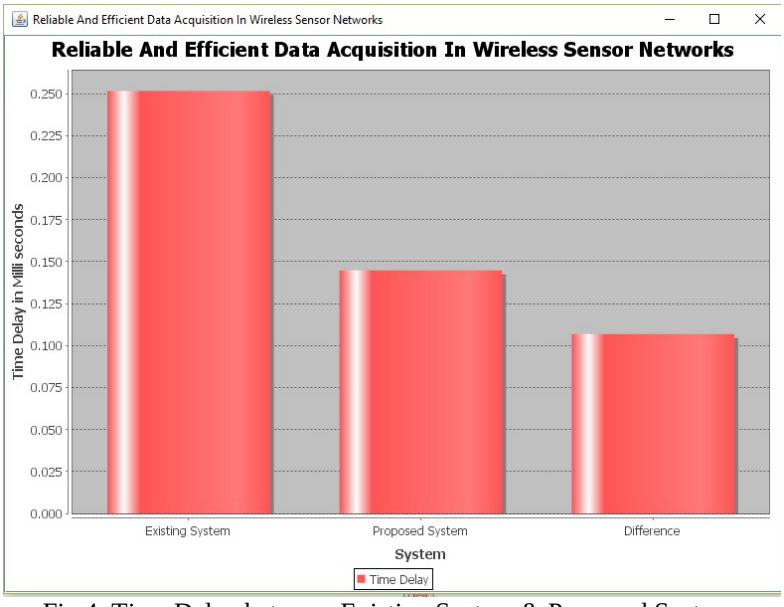


Fig 4. Time Delay between Existing System & Proposed System.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

VI. RESULTS

Sink node accept the data only when the data packet is not altered and also from transfaulty node. This can be achieved by using dual mode of communication i.e. acoustic and RF mode of communication with hash value.

VII. CONCLUSION

Consistent and effective WSN is essential of the today's communication technology and has been capable to capture the consideration of a number of scholars. The double mode working of the sensor nodes in the WSN has been capable to decrease the delay. Similarly the lifespan is enlarged by not removing the nodes straight when then go in the separation state. Energy of the node being one of the some essential issues, has to be worked upon by monitoring and with the help of the facts picked up by the survey. It also encourages to cogitate the moveable nodes and not just the immobile nodes and we can increase the computational power by ideal sensor placement in wireless sensor network. We also considered the issue of security by checking for the data packet at sink node with the hash value. This will allow a secure consistent and effective data acquisition in wireless sensor network in the presence of transfaulty node. In future, we going to use encryption for the data packet which is sensed by the sensor node.

REFERENCES

[1] Pushpendu Kar, Student Member, IEEE and Sudip Misra, Senior Member, IEEE, Reliable and Eficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes,IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, 8th Jan, 2016.
[2] Kealan McCusker, Noel E. O^aConnor, Low-energy symmetric key distribution in wireless sensor networks, IEEE Transactions on Dependable and Secure Computing May/June 2011.
[3] Cesare Alippi, Fellow, IEEE, Giuseppe Anastasi, Mario Di Francesco, and Manuel Roveri, Adaptive Sampling Algorithm for Efective Energy Management in Wireless Sensor Networks With Energy-Hungry Sensors, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 2, FEBRUARY 2010.
[4] Levente Buttya , LaAszlo Czap, and Istvan Vajda, Detection and Recovery from Pollution Attacks in Coding-Based Distributed Storage Schemes, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 6, NOVEMBER/DECEMBER 2011.
[5] Ing-Ray Chen, Member, IEEE, Anh Phan Speer, and Mohamed Eltoweissy, Senior Member, IEEE, Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL.8, NO. 2, MARCH-APRIL 2011.
[6] Masanori Miyazawa and Michiaki Hayashi Rolf Stadler, vNMF: Distributed Fault Detection using Clustering Approach for Network Function Virtualization, 2nd Jan, 2015.
[7] Steven S. McClure, L. D. Edmonds, R. Mihailovich, A. H. Johnston, Fellow, IEEE, P. Alonzo, J. DeNatale, Member, IEEE, J. Lehman, and C. Yui, Radiation Effects in Micro-Electromechanical Systems (MEMS): RF Relays, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 49, NO. 6, DECEMBER 2002.
[8] Erfan Soltanmohammadi, Student Member, IEEE, Mahdi Orooji, Student Member, IEEE, and Mort Naraghi-Pour, Member, IEEE, Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 1, Jan 2013.
[9] Tapas Kanungo, Senior Member, IEEE, David M. Mount, Member, IEEE, Nathan S. Netanyahu, Member, IEEE, Christine D. Piatko, Ruth Silverman, and Angela Y. Wu, Senior Member, IEEE, An Eficient k-Means Clustering Algorithm: Analysis and Implementation, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 24, NO. 7, JULY 2002.
[10] Vibha Paradkar, Gajendra Singh Chandel, Kailash Patidar, Fault Node Discovery and Eficient Route Repairing Algorithm for Wireless Sensor Network (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1710-1715.
[11] Saad Ahmad Khan, Ladislau B~ Ani, Damla Turgut, Bridge protection algorithms A technique for fault-tolerance in sensor networks Ad Hoc Networks 24 (2015) 186-199.
[12] Anasane, Aboli Arun, and Rachana Anil Satao. "A Survey on Various Multipath Routing Protocols in Wireless Sensor Networks." Procedia Computer Science 79 (2016): 610-615.
[13] Lathies Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks", IET Inf. Secur., 2014, Vol. 8, Iss. 1, pp. 1–7 doi: 10.1049/iet-ifs.2013.0133.
[14] Hevin Rajesh Dhasian, Paramasivan Balasubramanian, "Survey of data aggregation techniques using soft computing in wireless sensor networks", IET Inf. Secur., 2013, Vol. 7, Iss. 4, pp. 336–342 doi: 10.1049/iet-ifs.2012.0292.
[15] Parli B. Hari, Dr. Shailendra Narayan Singh," Security Issues in Wireless Sensor Networks: Current Research and Challenges", 978-1-5090-0673-1/16/$31.00 ©2016 IEEE.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

BIOGRAPHY

Mr.Chetan R. Patil is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. He received his B.E (Computer) Degree from Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411007. His area of interest is network security, WSN.

Prof. Madhav D. Ingle Pursing PhD from K L University. Received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad-402103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. SPPU, Pune, Maharashtra, India - 411007. His area of interest is network security and WSN.

Prof S. H. Patil Received her M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from College of Engineering, Ambejogai, India. BAMU, Maharashtra, India.She is currently working as Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. SPPU, Pune, Maharashtra, India - 411007. Her area of interest is networking, WSN.