ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Enhanced Security in Wireless Sensor Networks by Using Contingent Delivery Algorithm

Sujanya Nalli
Department of Computer Science Engineering,
Swarnandhra College of Engineering & Technology,
JNTUK, East Godavari, India.

Saka Umamaheswara Rao
Department of Computer Science Engineering,
Swarnandhra College of Engineering & Technology,
JNTUK, East Godavari, India.

Abstract:

Security has become one of the major issues for data transfer over wired and wireless networks. Compromise node (CN) and Denial of service (DOS) are two key attacks in wireless sensor networks. These both types of attacks can generate black holes. Data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that different classic multipath routing approaches are in a weak position to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm it can compute the same routes know to the source, hence, making all information sent over these routes vulnerable to its attacks. We considered the mechanisms that generate randomized or contingent multipath routes. Part of the charm of the proposed routing algorithm is taken by the shares of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot find out all the routes traversed by each packet. The experimental results clearly show the great advantages of the new routing algorithm for small-scale wireless sensor networks.

Keywords: Compromise node (CN), Randomized multipath routing, wireless sensor network, secure data delivery

1. INTRODUCTION:

The one of the high influential technology in the 21st century, Wireless Sensor Networks (WSNs) are extremely changing the human life. It is composing of lot of sensor nodes which contain sensing, computing the information and communication elements. The characteristics of WSN are limited energy capacity, low memory and minimum processing capabilities. The development of technology and economy, and the continuous improvement of living standards, the application scopes of WSNs become wider and wider, especially, the application of Small-scale Wireless Sensor Networks, which consists number of sensor nodes. The wide range of applications are involved with both civilian and military scenarios, including environmental monitoring, surveillance for safety and security, automated health care, intelligent building control, traffic control and object tracking, etc. [1]. With the development of computer hardware technology, the CPU and flash memory are becoming smaller and smaller, more and more powerful and cheaper and cheaper. As a result, the memory and processing capabilities of sensor nodes will not be the most important obstacle for the application of WSNs [2]. However, the battery technology has failed to obtain a breakthrough. Obviously, the energy capacity has become the key bottlenecks for the development of WSNs. So the research on energy efficiency of WSNs is still the focus. Therefore, many routing schemes used for MANETs are inappropriate for WSNs. For the wide applicability range of WSNs, it is impossible to build a WSN routing algorithm that fulfils all application requirements [3].

Instead it is of importance that designing general routing algorithms which somehow can be applied to some applications and meanwhile balance the energy consumption to increase the network lifetime as far as possible. Currently, there are great deals of research, as well as efforts that are on the go, for the development of routing protocols in WSNs. Next we are giving a brief overview on the application of applying intelligent optimization algorithms to develop routing protocols for WSNs. For a detailed and complete reference on the motif, please refer to [4], [5]. Energy Efficient Ant Based Routing Algorithm is proposed in wireless sensor networks to improve the energy efficiency of WSNs, so as to maximize the network lifetime [6]. In this routing algorithm, forward ants are launched to find paths between source nodes and sink node, where forward ants select next hop nodes based on the amount of pheromone trail stored in current node's routing table and residual energy of neighbours.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In the phase of calculating the number of pheromone trail that a backward ant will left during its journey, both the energy levels and the length of path are taken into consideration, which can contribute to balance the energy consumption and reduce the length of path. What's more, a parameter called travelled distance, i.e., the number of visited nodes, is introduced in this phase, which make those nodes closer to sink node will have more pheromone trail, so that forward ants could reach sink node more efficiently. However, it didn't provide the setting method of parameter. It is difficult to find an appropriate value to ensure the selection probability of some nodes are not so low, so some other nodes are easier to run out of energy for serving as router frequently [7]. Routing using ant colony optimization router chip proposed by Okdem and Karaboga is a multipath routing protocol, which provides reliable communications in the case of node faults. What's more, the packets to be transmitted don't need to retain those nodes that have been visited, so that the size of data has been decreased and nodes energy has been saved [8]. However, in the phase of calculating the amount of pheromone trail that a backward ant will deposit during its journey, it only consider the length of path but the energy levels of path, so that the distribution of pheromone are not so reasonable, which will have a negative effect on maximizing network lifetime [9].The paper is organized as follows: In the next section, some related concepts about Wireless Sensor Networks, In section 3 provides Randomized multipath Routing Algorithms. In section 4 experiment results of proposed algorithm is presented. In section 5 describes conclusions and future work.

2. RELATED WORK:

During the past decade, WSNs have seen increasingly intensive adoption of advanced machine learning techniques. In a short survey of machine learning algorithms applied in WSNs for information processing and for improving network performance was presented. A related survey that discussed the applications of machine learning in wireless ad-hoc networks The applications of three popular machine learning algorithms (i.e., reinforcement learning, neural networks and decision trees) at all communication layers in the WSNs. In contrast, specialized surveys that touch on machine learning usage in specific WSN challenges have also been written. For instance, [10], [11] addressed the development of efficient outlier detection techniques so that proper actions can be taken, and some of these techniques are based on concepts from machine learning. Meanwhile, [12] discusses computational intelligence methods for tackling challenges in WSNs such as data aggregation and fusion, routing, task scheduling, optimal deployment and localization. Here, computational intelligence is a branch of machine learning that focuses on biologically-inspired approaches such as neural networks, fuzzy systems and evolutionary algorithms [13].Generally, these early surveys concentrated on reinforcement learning, neural networks and decision trees which were popular due to their efficiency in both theory and practice. In this paper, we decided instead to include a wide variety of important up-to-date machine learning algorithms for a comparison of their strengths and weaknesses. In particular, we provide a comprehensive overview which groups these recent techniques roughly into supervised, unsupervised and reinforcement learning methods. Another distinction between our survey and earlier works is the way that machine learningtechniques are presented. Our work discusses machine learning algorithms based on their target WSN challenges, so as to encourage the adoption of existing machine learning solutions in WSN applications [14]. Lastly, we build on existing surveys and go beyond classifying and comparing previous efforts, by providing useful and practical guidelines for WSN researchers and engineers who are interested in exploring new machine learning paradigms for future research [15]. Previous contingent multipath routing algorithms in WSNs have not been designed with security issues in mind, largely due to their low energy efficiency. To the best of our knowledge, the work presented in this paper fills a void in the area of secure randomized multipath routing. Specifically, flooding is the most common randomized multipath routing mechanism. In flooding, every node in the network receives the packet and retransmits it once. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm [9] was proposed as a form of controlled flooding, whereby a node retransmits packets according to a pre assigned probability.

3. ENERGY EFFICIENT RANDOMIZED MULTIPATH DELIVERY:

In the Proposed System we are addressing efficient redundancy management of a clustered WSN to unreliable and malicious nodes which are responsible for packet loss. We are addressing the balance between energy consumption with the QoS requirement to gain in reliability and timeliness as well as to increase security

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

so that we can maximize the lifetime of a clustered WSN, it will also be a satisfying application for QoS requirements in case of multipath routing [16], [22]. In our work we have considered redundancy management of multipath routes which are based on trust and energy values and it is used for intrusion detection, and to maximize the system lifetime of a WSN in the presence of unreliable and malicious nodes. Today's research challenge in WSNs is coping with low power communication. Routing protocols in this regard plays a key role in efficient energy utilization. In sending data from sensor nodes to BS there is need to select a specific route and must be a shortest route, which mange to minimize the energy consumption is necessary [17], [18].

Hence we are using clustering approach to minimize the energy consumption. In this paper we are using symmetric encryption technique to protect confidentiality [5]. To increase security we have revealed more extensive attacks by the malicious nodes such as packet loss attack and jamming attack each assault is having altered energy requirement as well as security and reliability. More specifically, we are analysing the optimal amount of redundancy in WSN through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the possibility to answer users query must be maximized while maximizing the system lifetime To tolerate intrusion through multipath routing, there are two major problems to solve first is how many paths to use and second is what paths to use [19].

We are concentrating on to report the how many paths to use to reach to the sink problem. Our approach is different from existing for the, what paths to use problem, in that we do not consider specific routing protocols and we are not using any feedback information to solve the problem. Rather, we are employing IDS by which intrusion detection is performed only locally so that there must be less energy conservation by the nodes in the network [20]. The compromised nodes are detected and the path through that node is ignored from the WSN. In this paper we decide which paths to use in order to tolerate residual compromised nodes that survive our IDS, so as to increase system useful lifetime of the WSN. In this paper we also discover more extensive malicious attacks in addition to packet loss and jamming attacks which occur because of malicious nodes, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

3.1 Proposed System Model:

The WSN consists of different types of sensors having different sensing capabilities. We have considered two types of sensor nodes, one is cluster head (CHs) and another is sensor node SNs. Cluster heads (CHs) are more superior than sensor Nodes (SNs) in consideration of energy as well as computational resources. We are using heterogeneous network in which each node is having more amount of resources [21].

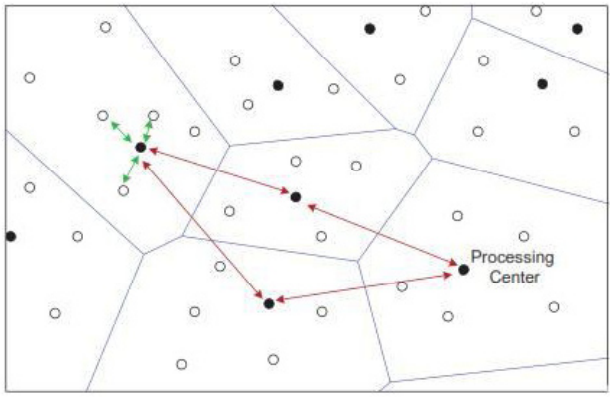

Fig.1. Cluster heads of a Wireless Sensor Network

Redundancy management of multipath routing for intrusion tolerance in presence of malicious nodes is achieved through two forms of redundancy: (a) source redundancy by which ms SNs sensing a physical phenomenon in the same feature zone are used to forward sensing data to their CH (referred to as the source CH); (b) path redundancy by which mp paths are used to relay packets from the source CH to the base station through the use of neighbouring CHs. Let us take the scenario with a source redundancy of 3 (m=3) and a path redundancy of 2 (m=2). It has been reported that the number of edge-disjoint paths between nodes is equal to the average node degree with a very high probability. Therefore, when the density is adequately high such that the average number of one-hop neighbours is sufficiently larger than mp and ms, we can effectively result in m redundant paths for path redundancy and mp distinct paths from m sensors for source redundancy [21]. We are assuming that geographic routing which is a well-known routing protocol for WSNs is used to route the data from CH to the base station or sink along with multipath routing; thus, in this case there is no need to conserve path information of the network. We must know the location of the destination node so that we can correctly send the packet towards it. So the CH are responsible to get the location of all SN and vice versa in its cluster and it is the part of clustering.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A CH is also aware with the location of neighbour CHs along with the direction towards the base station or sink. In this paper we are using clustering to reduce the energy consumption by the nodes to send data to the base station. Cluster is the group of Nodes and in the paper, we are grouping the nodes to form cluster. Here cluster formation is based on the specific region and the nodes located in the specified region. We are selecting the region with specific distance from the base station and then the area is selected and the nodes inside region are located and grouped. In this approach clusters are formed statically at the time of network deployment so all the sensor nodes and their CH nodes are selected. The Cluster Head is selected on the Highest Energy basis, the node which has maximum energy is selected as Cluster Head. We also assume that all the sensor nodes and cluster heads should operate in power saving mode so that less energy is utilized. Hence, a sensor is either active i.e. transmitting or receiving or it is in sleep mode. For the energy consumption while sending & receiving information we are using the energy model in for both CHs and SNs. To preserve confidentiality we are using AES symmetric key encryption algorithm. AES is Symmetric key Cryptographic algorithm [21]. It is used to provide security in our paper. While sending data, a sensor node can encrypt data by using key encryption technique and then send that encrypted data to the CH so that it is helpful to achieve confidentiality and authentication. Then the data is transmitted and it will help to secure data from the attacker and packets are formed from the file and actually packets are transmitted. At the destination the data is decrypted by the destination node.

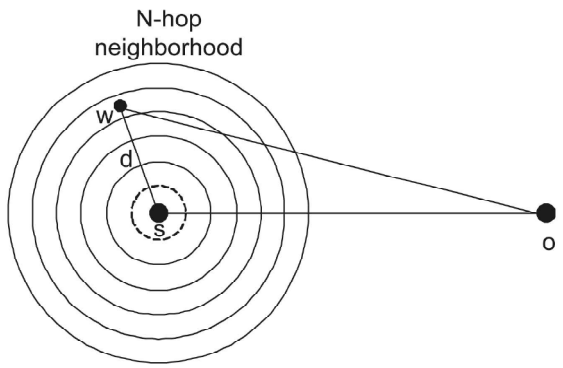

Fig.2. The total transmission distance after random propagation.

Let us assume that the energy consumption for delivering one bit over one hop is a constant q. Then, the average energy consumption for delivering one packet from source s to sink o depends on the average length (in hops) of the route. Note that each random route consists of two components. The first is a fixed N-hop component attributed to the random propagation operation. The second component involves sending the share from the last random relay node, i.e., w, to the sink o using a normal single path routing. Suppose w is located in the i th ring. Let the distance between w and s be (i-1) Rh ≤ d ≤ iRh. Given that the angle between sw and so be _, the distance between Sw and S0 is given by

$$Dw0(i)\ (d,\theta) = \sqrt{d2+ds2 - 2dds \cos \theta}\ .$$

Therefore, the unconditionally average distance between w and o is given by the weighted sum of Dw0(i) with weights Pr={€=i}, i.e,

$$Dw0 = \sum Ni=1\ Dw0(i)\ \ Pr=\{€=i\}.$$

Where the distribution of € has been obtained, When min-hop routing is used in the third phase, the number of hops from s to o can be approximated by ds / Rh. Let the lengths of an information packet and a share generated by the secret sharing algorithm be Lp and Ls, respectively.To detect compromised nodes from, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The acknowledge ACK which is received is compared with the size of received data; if it is equal then data is forwarded successfully with no loss in packets; otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens.

This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN. To detect jamming attack in network we are using a counter based approach if the counter goes beyond the threshold then it will detect that network is jammed. Here we have noted that increasing source redundancy as well as path redundancy will be described the reliability and security [22].

3.2. Algorithm for Intrusion Tolerance & attack detection:

The following algorithm shows to find the intrusion detection in wireless sensor networks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1. if (network created)
2. if (Source Node != Destination Node)
3. int Size = data size;
4. Send (data)
5. ACK = data received size;
6. if (ACK == data size)
7. Data received successfully;
8. Flag = true;
9. else
10. Data is lost in path;
11. Flag = false;
12. if(Flag == false)
13. For all paths;
14. Calculate average of energy and trust value
15. if (average==maximum value)
16. Shortest path = Current path;
17. Send (data);

In proposed work, we are using multipath routing and encryption/Decryption technique. The fundamental obligation of the sensor nodes in each system is to sense the range and transmit their gathered data to the sink node for further operations. Multipath Routing is a routing procedure, which chooses various ways to convey information in the middle of source and destination nodes. As the essential significance ofrouting means, selecting best way in the system, multipath routing strategies are utilized to choose the best path in the network.

From the above algorithm, Firstly a network is created which consist of different clusters and based on energy levels of each node the cluster heads are elected. To forward a data within a distinct source node and destination nodes are selected. To increase system lifetime we have to detect malicious nodes which are responsible for different attacks such as packet lossand jamming attack.

To detect compromised nodes from WSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The ACK is compared with the size of received data; if it is equal then data forwarded-successfully with no loss in packets, otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens. This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN [23] [25].

4. RESULTS AND DISCUSSION:

The aim of our system is to increase lifetime and security in the network. To evaluate the performance we need to use different metrics. In our work we are using following metrics: (1) Data Transfer Time (2) Data Delivery Ratio. The following graph of data transfer time required for communication, in this graph we shows three types of communication with Jamming, with MIM attack and with Normal communication and the time required for the communication. Lifetime is depending on the Energy of the network and as the energy consumption depends on the node processing time.

The jamming attack and MIM attack requires more time for processing and it consumes more energy and If we are using the same path for communication then we are wasting unnecessary energy and hence node may cause dead hence to avoid this we are changing the path and after the path change the data transfer time is less as compared to attack. Hence the minimum time requires minimum energy and indirectly the network lifetime is increased by path changed for communication.

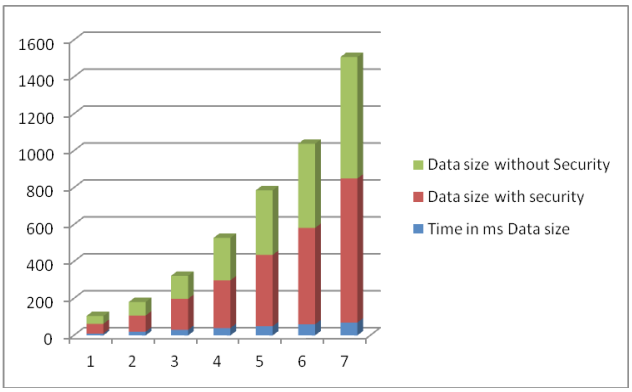

Fig.3. Data Delivery Ratio in Wireless Sensor Networks

The aim of our system is to increase lifetime and security in the network, in the first graph we shows that how we increased lifetime and this graph shows the time required for sending the specific size of data with and without security, as we are providing the security the time should be more as compared to normal sending for security we are using the encryption algorithm for security [24].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

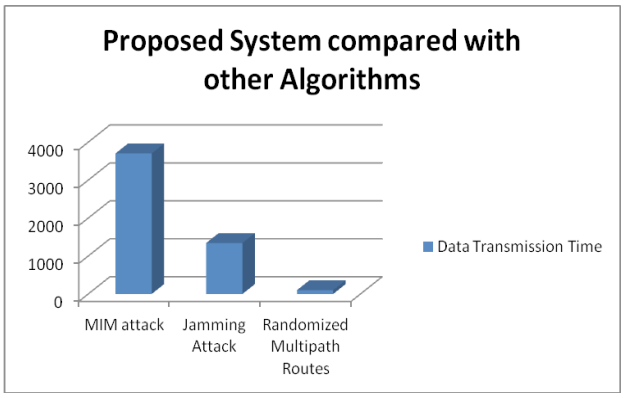

Fig.4.The Comparison of different algorithms based on data transmission time.

5. CONCLUSION:

In this paper we have performed a trade off analysis of energy consumption and QoS requirement to reliability gain and timeliness as well as to provide security for redundancy management of clustered wireless sensor networks by utilizing multipath routing to answer user queries. In our work, we consider redundancy management of multipath routes, based on trust and energy values, for intrusion detection, and to maximize the system lifetime of a WSN in the presence of unreliable and malicious nodes. We have noted that increasing source redundancy as well as path redundancy will enhance the reliability and security. However, it also decreases the energy consumption and thus it contributing to the increase of the system lifetime. Moreover, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counterparts. The proposed algorithms can be applied to some of selective packets in WSNs to describe additional security levels against adversaries attempting to acquire these packets. The random propagation and secret sharing different security levels can be provided by our algorithms at different energy costs and different efficiencies. This work is based on the assumption that there are only a small number of black holes in the WSN. In fact, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink. Adding with each other, these black holes can form a cut around the sink and can block every path between the source and the sink. Under this cut around- sink attack, no secret share from the source can escape from being intercepted by the adversary. Our current work does not address this attack. But future work is to extend our mechanisms to handle multiple collaborating of all black holes in wireless sensor networks.

REFERENCES:

[1] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp.560–563, 2007.

[2] J. B. Predd, S. Kulkarni, and H. V. Poor, "Distributed learning in wireless sensor networks," IEEE Signal Process. Mag., vol. 23, no. 4, pp. 56–69, Jul. 2006.

[3] C.S. Raghavendra, K.M. Sivalingam, T. Znati, Wireless sensor networks, Springer, 2004.

[4] N.A. Pantazis, S.A. Nikolidakis, D.D. Vergados, Energy-efficient routing protocols in wireless sensor networks: A survey, Communications Surveys & Tutorials, IEEE, 15 (2013) 551-591.

[5] Gudikandhula Narasimha Rao, P.Jagadeeswara Rao, "A Clustering Analysis for Heart Failure Alert System Using RFID and GPS", 48th Annual Convention Computer Society of India, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II, Springer, Advances in Intelligent Systems and Computing, Volume 249, 2014, pp 729, CSI 2013, Visakhapatnam, Andhra Pradesh, India, 13th -15th December, 2013.

[6] W. Guo, W. Zhang, A survey on intelligent routing protocols in wireless sensor networks, Journal of Network and Computer Applications, 38 (2014) 185-201.

[7 J. Yang, M. Xu, W. Zhao, B. Xu, A multipath routing protocol based on clustering and ant colony optimization for wireless sensor networks, Sensors, 10 (2010) 4521-4540.

[8] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002AI Magazine, vol. 18, no. 4, pp. 97–136, 1997.

[10] P.C. Lee, V. Misra, and D. Rubenstein, "Distributed Algorithms for Secure Multipath Routing," Proc. IEEE INFOCOM, pp. 1952- 1963, Mar. 2005.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[11] W. Lou and Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.

[12] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 2002.

[13] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[14] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. ACM MobiHoc, 2005.

[15] E. Felemban, L. et al, "MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol.5, no. 6, pp.738–754.

[16] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh.Technol. Conf., pp. 2528–2532.

[17] G. Narasimha Rao, R. Ramesh, D. Rajesh, D. Chandra sekhar."An Automated Advanced Clustering Algorithm For Text Classification". In International Journal of Computer Science and Technology, vol 3,issue 2-4, June, 2012, eISSN : 0976 - 8491,pISSN : 2229 – 4333.

[18] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

[19] Y. Zhou, Y. Fang, et.al., "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[20] Rajesh Duvvuru, Sunil Kumar Singh, G. Narasimha Rao, Ashok Kote, B.Bala Krishna and M.Vijaya Raju . "Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA". Title: Heterogeneous Networking for Quality, Reliability, Security and Robustness, QSHINE 2013, SPRINGER, LNICST 115, pp. 185-196, 2013. © Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2013. ISBN- 978-3-642-37948-2.

[21] B. Balaji Bhanu , Dr. P. Srinivasulu, Gudikandhula Narasimha Rao,"Secure Group Key Communication in Sensor Networks" In International Journal of Advanced Computer Engineering and Arcitecture, Vol. 2 No. 1 (January-June,2012) ISSN: 2248-9452.

[22] G. Narasimha Rao, R. Ramesh, D. Rajesh, D. Chandra sekhar."An Automated Advanced Clustering Algorithm For Text Classification". In International Journal of Computer Science and Technology, vol 3,issue 2-4, June, 2012, eISSN : 0976 - 8491,pISSN : 2229 – 4333.

[23] Duvvuru, Rajesh, P. Jagadeeswara Rao and Gudikandhula Narasimha Rao. "Multi-Level Chaos Based Encryption Mechanism to Enhance Security of High Security Zone Areas on Google Map Satellite Images of India." International Journal of Applied Engineering Research 10.3 (2015): 8059-8072.

[24] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in Proc. 2006.

[25] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipathscheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, 2006.

[26] N. Kimura and S. Latifi, "A survey on data compression in wireless sensor networks," in Proc. Int. Conf. Inf. Technol., Coding Comput., 2005, vol. 2, pp. 8–13.