Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Network Pre-Failure Recovery Scheme for Distributed and Secured Wireless Sensor Network

Nukala Sudheer Kumar
M.Tech,
Dept of CSE,
VBIT College, Vidya Nagar, Proddatur.

P.Narasimhaiah
Assistant Professor,
Dept of CSE,
VBIT College, Vidya Nagar, Proddatur.

Abstract:

A wireless detector network consists of little detector nodes, that is capable of assembling info from the surroundings and communicating to the controller via wireless transceivers. Limited battery energy is employed to control the detector nodes and is extremely troublesome to exchange or recharge it, once the nodes die. It is often difficult or not possible to exchange the batteries of the detector nodes. On the opposite hand, the final destination is often rich in energy. Since the detector energy is that the most precious resource within the WSN, effective utilization of the energy to improve the network period has been the main focus of abundant of the analysis on the WSN. This can have an effect on the network performance. In most of existing protocols authors considered only on the centralized data dissemination methods without more security and energy consideration.

We have a tendency to establish the safety vulnerabilities in previously planned protocols and that we extend the secured and distributed information delivery system with energy concerns. It's the first distributed information discovery and dissemination protocol that permits network owners and approved users to disperse information items into WSNs without hoping on the base station and with network life time management. The existing DiDrip [1] protocol is only concentrating on the security point. In our project we propose as enhanced dissemination protocol, which is used to improve the quality of service issues. In our enhanced work we propose a solution to enhance the energy efficiency in distributed wireless sensor network.

Keyword:

WSN, Energy, Security, Attacks, Data dissemination.

1.Introduction:

The communications within the WSN has the many-to-one property in this information from a large number of detector nodes tend to be targeted into one sinks. Since multi-hop routing is usually required for distant detector nodes from the sinks to save huge amount of energy, the devices close to a sink are often loaded with relaying an over-sized quantity of traffic from different nodes. Detector nodes resources affected in term of energy, processor and memory and low vary communication and information measure. The detector nodes are commonly expected to work with batteries and they are usually deployed to not-easily-accessible or hostile surroundings, generally in giant quantities. Routing is a crucial issue in information gathering detector network, whereas on the opposite hand sleep/wake maintenance is that the main problems for event detection networks. Even though, we cannot avoid the failure of nodes, so in our research work, further we added the enhancement with the failure rectification techniques. Our ultimate aim of this project is to provide the energy efficient distributed security system for WSN. And more importantly, all previous data discovery & dissemination algorithms employ the centralized method.

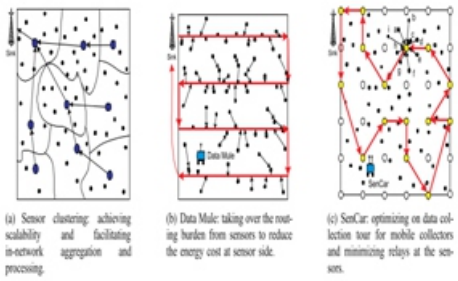

Fig.1 Mobility in sensor network

We propose EDiDrip to make higher life time in data dissemination method, another possible approach to authentication is by single key cryptography.

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

But, this type of method is vulnerable to device compromise attack because once a device is attacked; the commonly shared secrets are revealed. . Shah et al. [1] investigated mobility underneath stochastic process wherever the mobile collector picks up information from close sensors, buffers and eventually offloads information to the wired access purpose. However, random phenomenon cannot guarantee latency bounds that area unit needed in several applications. In [2], Jea et al. more projected to manage information mules to traverse the sensing field on parallel straight lines and collect information from close sensors with multi-hop transmissions as shown in Fig. 2b.

This theme works well in an exceedingly uniformly distributed detector network. to attain additional versatile information gathering tour for mobile collectors, Ma associate degreed principle [6] projected an economical moving path designing algorithmic program by decisive some turning points on the straight lines, that is accommodative to the detector distribution and might effectively avoid obstacles on the trail. In [1], they instead projected a single-hop information gathering theme to pursue the right uniformity of energy consumption among sensors (see Fig. 1c), wherever a mobile collector referred to as SenCar is optimized to prevent at some locations to collect information from sensors within the proximity via single-hop transmission. Secured visibility hides data from anything outside the class division. Common visibility allows all other classes to see the marked data.

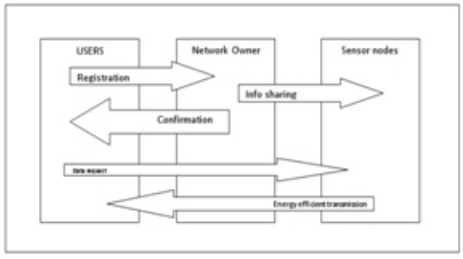

Fig.2 Security architecture

The protected visibility gives the permission child classes to access data they inherited from a parent class. In our project work all the attributes are kept in the private info. Fig.2 shows the our proposed security architecture

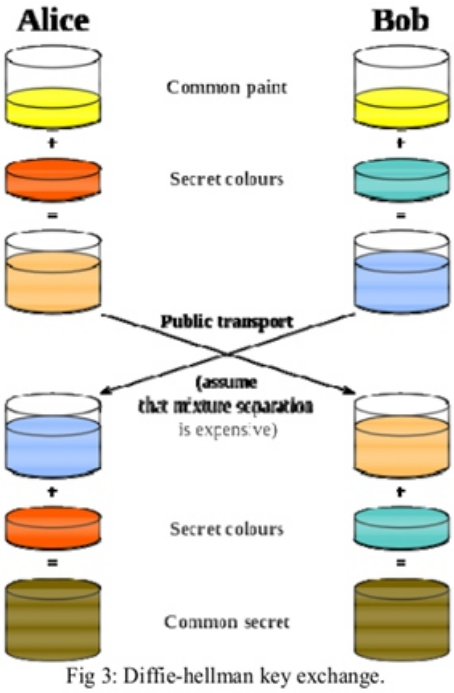

Fig 3: Diffie-hellman key exchange.

2.Related Work:

The existing DiDrip [1] protocol is only concentrating on the security point. In our project we propose as enhanced dissemination protocol, which is used to improve the quality of service issues. In our enhanced work we propose a solution to enhance the energy efficiency in distributed wireless sensor network. In the literature, many of data discovery and dissemination algorithms [3] to [6] have been proposed for WSNs. Some of them, DIP [5], DHV [3] and Drip [4] are stated as the state-of-the-art algorithms and have been included with in the TinyOS. Most of proposed algorithm assumes that the operating environment of the WSN is trustable and has no malicious. But, in actual, malicious exist and impose security problems to the normal operation of wireless sensor network [8]. The security problem has only been rectified recently by [7] which identifies the security vulnerabilities of Drip and proposes an effective solution. But there is no consideration with energy issues. So in our proposed work we have followed these types of existing protocols and extended the work to the energy efficient routing and energy based trusting system. And the paper [9] describes the energy efficient routing in centralized network. We propose a energy efficient routing for the distributed network. There has been lot of connected research on the failure detection problem [10], [11], [12].

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Authors in [10] studied the matter of detecting topological holes in WSN with no localization info. They gave a distributed theme that's supported the communication topology graph. A node decides whether or not it's on the boundary of a hole by comparison its degree with the typical degree of its 2-hop neighbors. Not all boundary nodes may be known properly by this formula. Indeed, for an outsized WSN with few holes this technique isn't efficient [10]. An algebraical topological technique mistreatment similarity theory detects single overlay coverage holes while not coordinates [11], [12]. Ghrist and Muhammad [4] utilized a central management formula that needs property info for all nodes within the RoI. the fundamental situation may be delineated as follows: throughout traditional operation of the network, a good loss of nodes happens, thanks to associate external attack for instance, inflicting the creation of 1 or many massive holes among the network creating it ineffective. Our drawback is to style a mechanism for detective work and convalescent holes by exploiting solely the nodes quality. It ought to be noted that solely the holes among the network are thought-about. The holes on the border that are the results of the initial readying aren't self-addressed. The work was more extended in [13] to optimize the information gathering tour by exploring the trade-off between the shortest moving tour of SenCar and therefore the full utilization of coincidental data uploading among sensors. Furthermore, Somasundara et al projected associate degree algorithmic program [14] to check the programming of mobile parts such there's no information loss owing to buffer overflow.

3.Proposed Solution:

The need of distributed information discovery and dissemination protocols isn't fully new, however previous work failed to address this need. We have a tendency to study the functional necessities of such protocols, and set their style objectives. Also, we have a tendency to establish the safety vulnerabilities in previously planned protocols and that we extend the secured and distributed information delivery system with energy concerns as well as the failure rectification techniques with proactive manner unlike previous report work (in previous work we researched the on demand solution work). It's the first distributed information discovery and dissemination protocol that permits network owners and approved users to disperse information items into WSNs without hoping on the base station and with network life time management by using the autonomous actor placement systems. In our project we propose as enhanced dissemination protocol, which is used to improve the quality of service issues. In our enhanced work we propose a solution to enhance the network life time in distributed wireless sensor network with pre-failure rectification technique. Our ultimate aim of this project is to provide the energy efficient distributed security system for WSN. And more importantly, all previous data discovery & dissemination algorithms employ the centralized method. We propose EDiDrip to make higher life time in data dissemination method, another possible approach to authentication is by single key cryptography. But, this type of method is vulnerable to device compromise attack because once a device is attacked; the commonly shared secrets are revealed. . This project proposes the first Energy efficient secure and distributed data discovery and dissemination protocol named EDiDrip. It provides the network owners to authenticate multiple network users with different categories to simultaneously and directly share data items to the detector nodes. An adversary can first place some intruder devices in the network and then use them to alter the data being share or forge a data item. This might result in some necessary parameters being deleted or the total network being restarted with wrong data.

3.1.Proposed work functional module:

EDiDrip consists of 5 modules (Fig.4), Network format, user connection, and packet preprocessing and packet verification and pre-failure healing process. In our base project work we have proposed the security solutions based on the energy availability monitoring. Wireless sensing element networks represent a new category of computing with massive numbers of resource-constrained computing nodes cooperating on basically one application. We tend to study the purposeful necessities of such protocols, and set their style objectives. Also, we tend to establish the safety vulnerabilities in antecedently projected protocols. 2) supported the planning objectives, we tend to propose EDiDrip. It's the first energy based distributed knowledge discovery and dissemination protocol, that permits network controllers and licensed users to spread knowledge sets into WSNs while not hoping on the BS, the route selection is based on the energy parameters.

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Moreover, our intensive analysis demonstrates that EDiDrip satisfies the safety necessities of the protocols of its kind. Particularly, we tend to apply the demonstrable security technique to formally prove the credibleness and integrity of the disseminated knowledge things in EDiDrip. 3) We tend to demonstrate the potency of EDiDrip in follow by implementing it in associate degree simulation experiment WSN with resource-limited sensing element nodes. System interface can comprise system components. It can provide action of plan from which software can be mad, and systems developed, that will work combine to implement the overall system. In this section, we are going to discuss about our enhancement work. Our base reference method works like reactive mode, if the device failed then only failure rectification will start (Fig.5). By our base work we can cover the holes, but reactive method may cause to high level location changes, and then more number of nodes has to move from own position. Due more number of node failure, the total network may not be rectified after certain healing process. Compared with data assortment via a static sink, introducing mobility for information assortment enjoys the advantages of equalization energy loss within the network and joining disconnected regions.

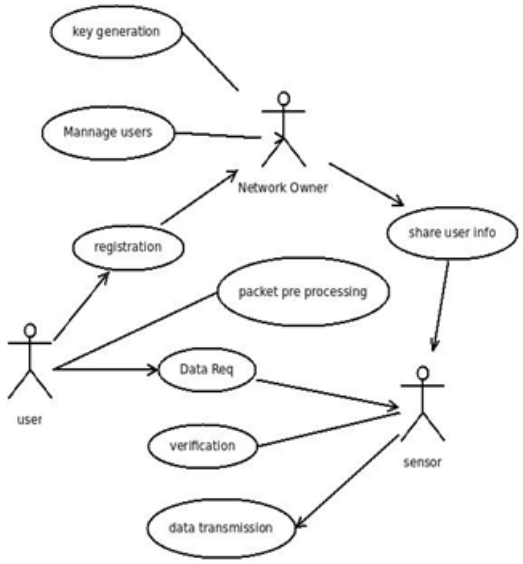

Fig.4 device interaction diagram

3.2.Algorithm: (failure rectification)

Let, E_c for Remaining energy level, E_{Th} for minimum energy level, L_{critic} for critical node list, L_{Exact} for Available Extra Mobile sensor list, Id_{Ex} for Extra Mobile sensor Id, Pos for postion,

1) If $E_c < E_{Th}$
   a. Generate $Pkt.critical$
   b. $Pkt.Nd = N_{id}$
   c. Broadcast Pkt
2) If Pkt recv in N
   a. If pkt is Duplicate
      i. Free Pkt
      ii. $Return$
   b. If $Pkt.critical$
      i. If $N \neq BS$
         1. Rebroadcast Pkt
      ii. If $N = BS$
         1. $Pkt.Nd \cup L_{critic}$
         2. If $L_{Exact} \neq Null$
            a. $Id_{Ex} = L_{Exact}(1)$
            b. $Rearrange(L_{Exact})$
            c. $Move(Id_{Ex} \rightarrow L_{Critic}(1).Pos)$
            d. $Rearrange(L_{Critic})$
   c. If $Pkt.Exact_{arrive}$
      i. If $N \neq Nd_{Crical}$
         1. $Ignore(Pkt)$
         2. $return$
      ii. $Switch_{neigh}(N \rightarrow Id_{Ex})$
      iii. $Move(N \rightarrow BS.pos)$

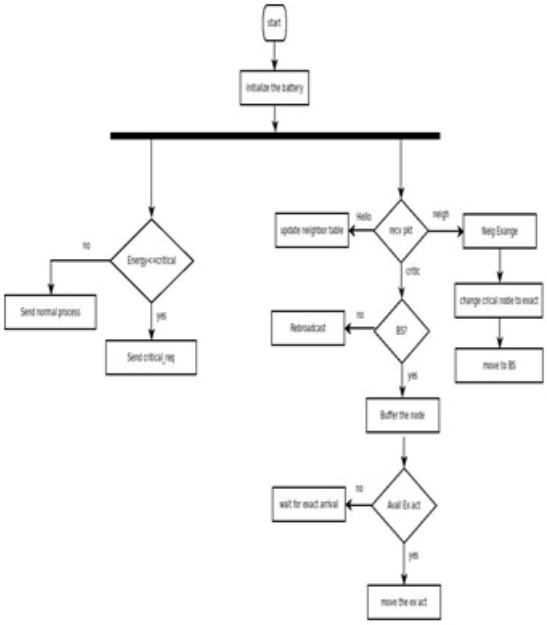

Fig.5 Failure rectifications

Result:

We have tested our output with ns2 simulator and we got a two results, one is NAM, Xgraph.

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Our enhancement method provides best results such as no node failure and less movement. The fig. 6 shows the basic network deployment with network owner, sensors and users.

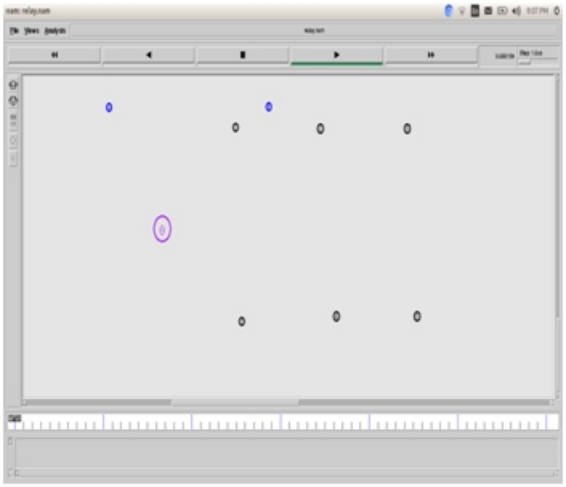

Fig.6 Network Placements

Fig.7 &8 shows that the registration key sharing of user with network owner

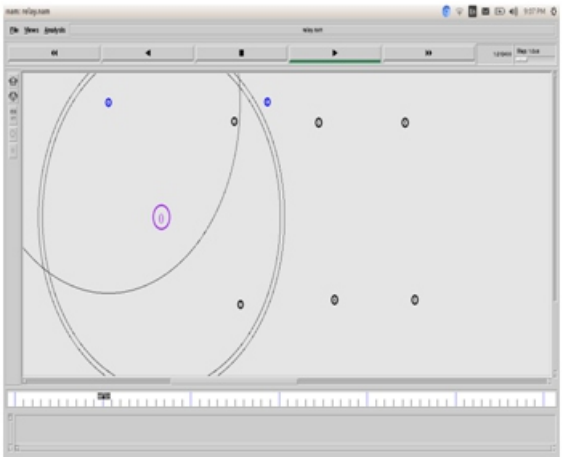

Fig.7 User registration process

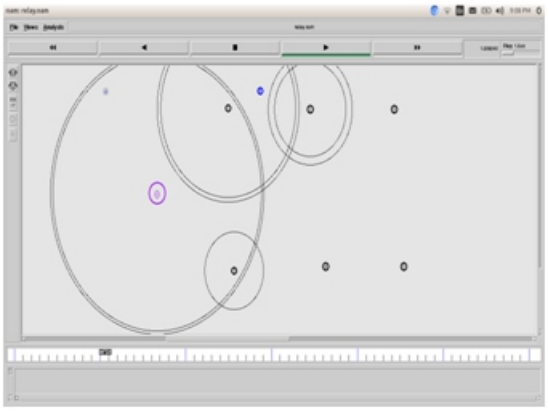

Fig.8 key sharing

Fig.9 shows the packet delivery from sensor to user after verification process

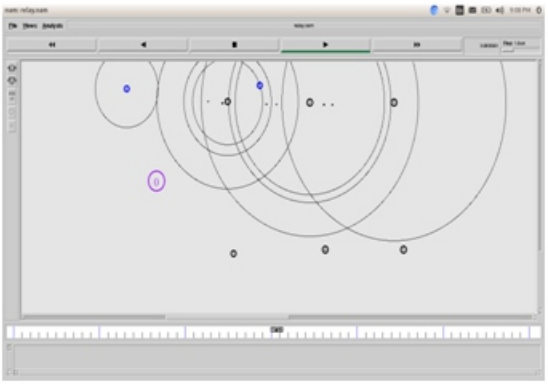

Fig.9 Secured Data transmission process

With security system we proposed the technique which uses the failure preprocessing technique, which can identify the failure in advance and exchange the node by the SensRob system. the xgraph shows the best of our rectification technique performance (fig 12 & 11)

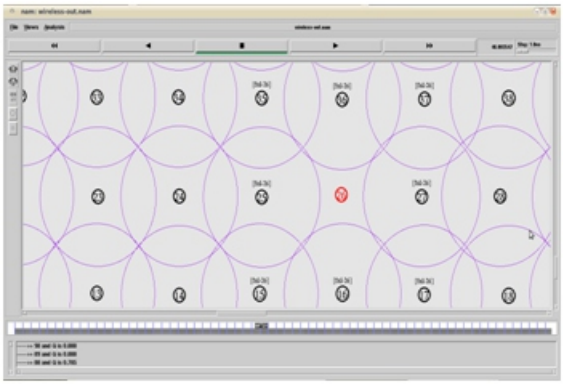

Fig.10 shows that the Failure detection and replacement system

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

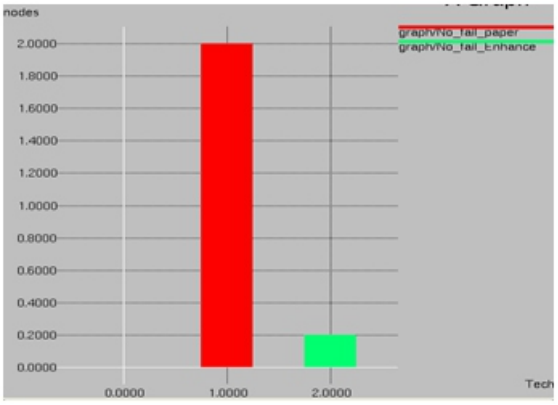

Fig.11 Failure comparison graph

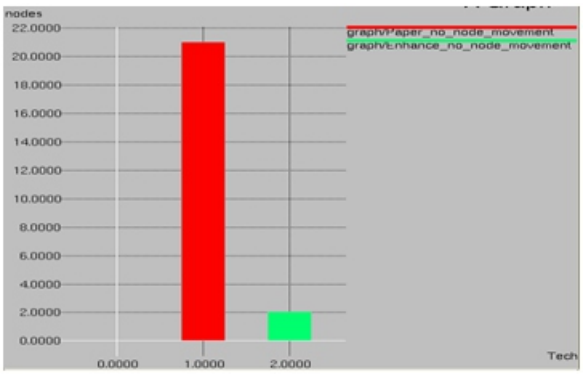

Fig.12. Node movement

Conclusion:

In most of existing protocols author considered only on the centralized data dissemination methods without more security and energy consideration. We have proposed the solution to establish the security protocol and that we extended the secured and distributed information delivery system with energy concerns. It's the first distributed information discovery and dissemination protocol that permits network owners and approved users to disperse information items into WSNs without hoping on the base station and with network life time management. From our tested results, we can conclude that our research work providing good energy efficient security architecture to wireless sensor network. In future, we will autonomous sensor robotic network to improve the disaster management system.

Reference:

[1] "Secure And Distributed Data Discovery And Dissemination In Wireless Sensor Networks", Daojing He, Member, Ieee, Sammy Chan, Member, Ieee, Mohsen Guizani, Fellow, Ieee, Haomiao Yang, Member, Ieee, And Boyang Zhou, Ieee Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.

[2] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012.

[3] T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.

[4] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Netw., 2005, pp. 121–132.

[5] K. Lin and P. Levis, "Data discovery and dissemination with DIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008, pp. 433–444.

[6] M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M. Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638– 4646, Sep. 2013.

[8] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE Global Telecommun. Conf., 2008, pp. 1–5.

[9] "designing energy routing protocol with power consumption optimization in manet", shivashankar1, hosahalli narayanagowda suresh2, golla varaprasad3, and guruswamy jayanthi4, ieee transactions on emerging topics in computing, 2013.

[10] N. Ahmed, S.S. Kanhere, and S. Jha, "The Holes Problem in Wireless Sensor Networks: A Survey," SIGMOBILE Mobile Computing Comm. Rev., vol. 9, no. 2, pp. 4-18, 2005.

Volume No:2, Issue No:1 (June-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[12] B. Wang, Coverage Control in Sensor Networks. Springer, 2010.

[13] B. Kun, T. Kun, G. Naijie, L.D. Wan, and L. Xiaohu, "Topological Hole Detection in Sensor Networks with Cooperative Neighbors," Proc. Int'l Conf. Systems and Networks Comm. (ICSN'06), p. 31, 2006.

[14] R. Ghrist and A. Muhammad, "Coverage and Hole-Detection in Sensor Networks via Homology," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), pp. 254-260, Apr. 2005.

[5] V. De Silva, R. Ghrist, and A. Muhammad, "Blind Swarms for Coverage in 2-D," Proc. Robotics: Science and Systems, pp. 335-342, June 2005.

[16] D. Jea, A. A. Somasundara, and M. B. Srivastava, "Multiple controlled mobile elements (data mules) for data collection in sensor networks," in Proc. IEEE/ACM Int. Conf. Distrib. Comput. Sensor Syst., Jun. 2005, pp. 244–257.

[17] M. Ma, Y. Yang, and M. Zhao, "Tour planning for mobile data gathering mechanisms in wireless sensor networks," IEEE Trans.

[18] Veh. Technol., vol. 62, no. 4, pp. 1472–1483, May 2013. M. Zhao and Y. Yang, "Bounded relay hop mobile data gathering in wireless sensor networks," IEEE Trans. Comput., vol. 61, no. 2, pp. 265–271, Feb. 2012.

[19] M. Zhao, M. Ma, and Y. Yang, "Mobile data gathering with space-division multiple access in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1283–1291.

[20] M. Zhao, M. Ma, and Y. Yang, "Efficient data gathering with mobile collectors and space-division multiple access technique in wireless sensor networks," IEEE Trans. Comput., vol. 60, no. 3, pp. 400–417, Mar. 2011.

[21]A. A. Somasundara, A. Ramamoorthy, and M. B. Srivastava,, "Mobile element scheduling for efficient data collection in wireless sensor networks with dynamic deadlines," in Proc. 25th IEEE Int. Real-Time Syst. Symp., Dec. 2004, pp. 296–305.

Author's Details:

Nukala Sudheer Kumar
received B. Tech (CSE) degree from Sri Venkateswara College of Engineering and Technology, Chittoor. and M.Tech (CSE) degree from the Vignana Bharathi Institute of Technology, Vidya Nagar, Proddatur. He is interested in wireless sensor network security protocol research work.

P. Narasimhaiah
received B.Sc (MPCS) Degree and M.Sc (CS) Degree from Sri Venkateswara University Tirupathi and M.Tech(CS) degree from JNTUA Anantapur. From 2001 to 2006 he worked as a Lecturer in Dept. of Computer Science ,Sri Varadaraja P G College, Proddatur. From 2006 to 2011 he worked as a Lecturer in Dept. of Master of Computer Applications, SVPG College, Kadapa. From 2011 to 2015 he worked as a Asst. Prof in Dept. of CSE ,C B I T Vidya Nagar, Proddatur. From 2015 to till date he worked as a Asst. Prof in Dept. of CSE, V B I T Vidya Nagar, Proddatur.