Network Pre-Failure Recovery theme for Distributed and secured Wireless sensing element Network

Alekhya K

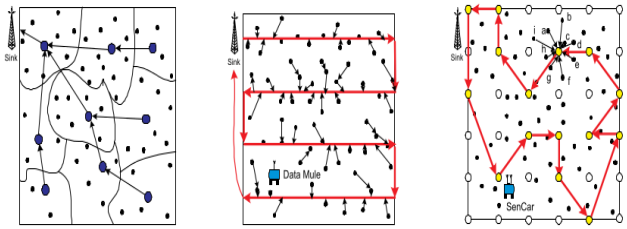
PG Scholar, Department of Master of Computer Applications, Hitech College of Engineering and Technologies, Moinabad, Hyderabad, Telangana, India.

Abstract **-** A wireless detector network consists of very little detector nodes, that's capable of grouping data from the environment and act to the controller via wireless transceivers. restricted battery energy is used to regulate the detector nodes and is extraordinarily difficult to exchange or recharge it, once the nodes die. it's usually tough or impossible to exchange the batteries of the detector nodes. On the alternative hand, the ultimate destination is commonly wealthy in energy. Since the detector energy is that the foremost precious resource among the WSN, effective utilization of the energy to boost the network amount has been the most focus of galore of the analysis on the WSN. this may have an impact on the network performance. In most of existing protocols authors thought of solely on the centralized knowledge dissemination strategies while not a lot of security and energy thought. we've got a bent to ascertain the protection vulnerabilities in antecedently planned protocols which we tend to extend the secured and distributed data delivery system with energy considerations. It's the primary distributed data discovery and dissemination protocol that allows network homeowners and approved users to disperse data things into WSNs while not relying on the bottom station and with network life time management. the present DiDrip [1] protocol is just concentrating on the safety purpose. In our project we tend to propose as increased dissemination protocol, that is employed to boost the standard of service problems. In our increased work we tend to propose an answer to boost the energy potency in distributed wireless device network.

Keywords **-** *WSN, Energy, Security, Attacks, Data dissemination.*

I. INTRODUCTION

The communications inside the WSN has the many-to-one property during this data from an oversized variety of detector nodes tend to be targeted into one sinks. Since multi-hop routing is typically needed for distant detector nodes from the sinks to save lots of vast quantity of energy, the devices near a sink square measure typically loaded with relaying associate over-sized amount of traffic from totally different nodes. Detector nodes resources affected in term of energy, processor and memory and low vary communication and knowledge live. The detector nodes square measure normally expected to figure with batteries and that they square measure typically deployed to not-easily-accessible or hostile surroundings, usually in large quantities. Routing may be a crucial issue in military operation detector network, whereas on the other hand sleep/wake maintenance is that the most issues for event detection networks. even if, we have a tendency to cannot avoid the failure of nodes, thus in our analysis work, any we have a tendency to additional the sweetening with the failure rectification techniques. Our final aim of this project is to produce the energy economical distributed security system for WSN. And additional significantly, all previous information discovery & dissemination algorithms use the centralized methodology.



(a) Sensor clustering: achieving scalability and facilitating in-network aggregation and processing.

(b) Data Mule: taking over the routing burden from sensors to reduce the energy cost at sensor side.

(c) SenCar: optimizing on data collection tour for mobile collectors and minimizing relays at the sensors.

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. 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.

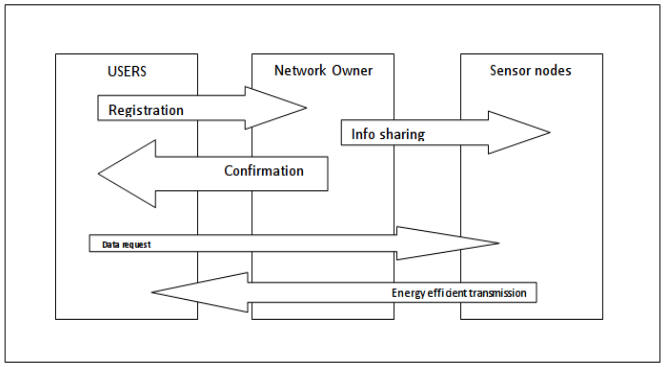


Fig.2 Security architecture

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

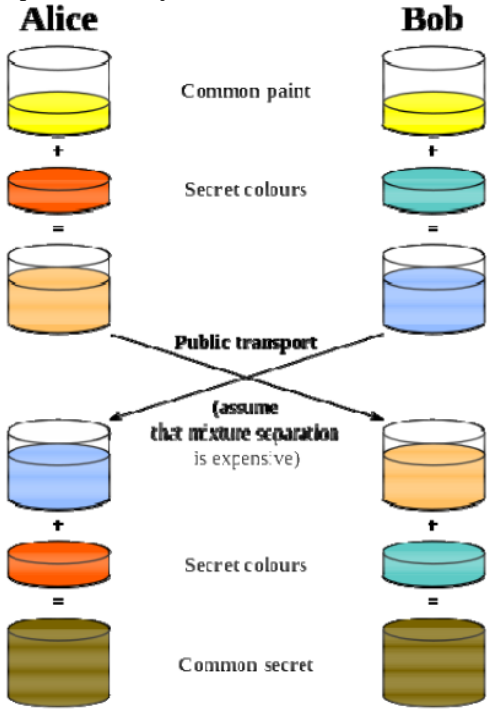


Fig 3: Diffie-hellman key exchange.

II. 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 enclosed with within the TinyOS. Most of projected algorithmic program assumes that the in operation atmosphere of the WSN is trustable and has no malicious. But, in actual, malicious exist and impose security issues to the traditional operation of wireless device network [8]. the safety downside has solely been corrected recently by [7] that identifies the safety vulnerabilities of Drip and proposes a good answer. however there's no thought with energy problems. thus in our projected work we've followed these sorts of existing protocols and extended the work to the energy economical routing and energy based mostly trusting system. and therefore the paper [9] describes the energy economical routing in centralized network. we tend to propose a energy economical routing for the distributed network. There has been ton of connected analysis on the failure detection downside [10], [11], [12]. Authors in [10] studied the matter of detection topological holes in WSN with no localization data. They gave a distributed theme that is supported the communication topology graph. A node decides whether or not or not it's on the boundary of a hole by comparison its degree with the everyday degree of its 2-hop neighbors. Not all boundary nodes is also legendary properly by this formula. Indeed, for associate degree large WSN with few holes this method is not economical [10].

An pure mathematics topological technique practice similarity theory detects single overlay coverage holes whereas not coordinates [11], [12]. Ghrist and Muhammad [4] utilised a central management formula that wants property data for all nodes at intervals the RoI. the basic state of affairs is also diagrammatical as follows: throughout ancient operation of the network, a decent loss of nodes happens, due to associate external attack for example, inflicting the creation of one or several large holes among the network making it ineffective. Our disadvantage is to vogue a mechanism for detecting and convalescent holes by exploiting entirely the nodes quality. It need to be noted that entirely the holes among the network square measure thought-about. The holes on the border that square measure the results of the initial activity are not addressed. The work was additional extended in [13] to optimize information} gathering tour by exploring the trade-off between the shortest moving tour of SenCar and thus the total utilization of concurrent 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.

III. PROPOSED SOLUTION

The need of distributed info discovery and dissemination protocols is not absolutely new, but previous work didn't address this want. we've got an inclination to review the purposeful requirements of such protocols, and set their vogue objectives. Also, we've got an inclination to determine the security vulnerabilities in antecedently planned protocols which we have a tendency to extend the secured and distributed info delivery system with energy considerations {as we have a tendency because the failure rectification techniques with proactive manner in contrast to previous report work (in previous work we researched the on demand answer work). It's the primary distributed info discovery and dissemination protocol that allows network house owners and approved users to disperse info things into WSNs while not wishing on the bottom station and with network lifetime management by victimization the autonomous actor placement systems. In our project we have a tendency to propose an increased dissemination protocol, that is employed to enhance the standard of service problems. In our increased work we have a tendency to propose an answer to boost the network lifetime in distributed wireless detector network with pre-failure rectification technique. Our final aim of this project is to produce the energy economical distributed security system for WSN. And additional significantly, all previous knowledge discovery & dissemination algorithms use the centralized methodology. we have a tendency to propose EDiDrip to create higher lifetime in knowledge dissemination methodology, another potential approach to authentication is by single key cryptography. But, this kind of methodology is prone to device compromise attack as a result of once a tool is attacked; the normally shared secrets area unit unconcealed. This project proposes the primary Energy economical secure and distributed knowledge 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.

A. Proposed work functional module

EDiDrip consists of five modules (Fig.4), Network format, user affiliation, and packet preprocessing and packet verification and pre-failure healing method. In our base project work we've got planned the protection solutions supported the energy accessibility watching. Wireless device networks represent a brand new class of computing with large numbers of resource-constrained computing nodes cooperating on essentially one application. we have a tendency to tend to review the purposeful wants of such protocols, and set their vogue objectives. Also, we have a tendency to tend to ascertain the security vulnerabilities in previously projected protocols. 2) supported the look objectives, we have a tendency to tend to propose EDiDrip. It's the primary energy based mostly distributed data discovery and dissemination protocol, that allows network controllers and authorised users to unfold data sets into WSNs whereas not looking forward to the baccalaureate, the route choice relies on the energy parameters. Moreover, our intensive analysis demonstrates that EDiDrip satisfies the security wants of the protocols of its kind. notably, we have a tendency to tend to use the demonstrable security technique to formally prove the credibility and integrity of the disseminated data things in EDiDrip. 3) we have a tendency to tend to demonstrate the efficiency of EDiDrip in follow by implementing it in academic degree simulation experiment WSN with resource-limited device nodes. System interface will comprise system elements. It will give action of set up from that software package is 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.

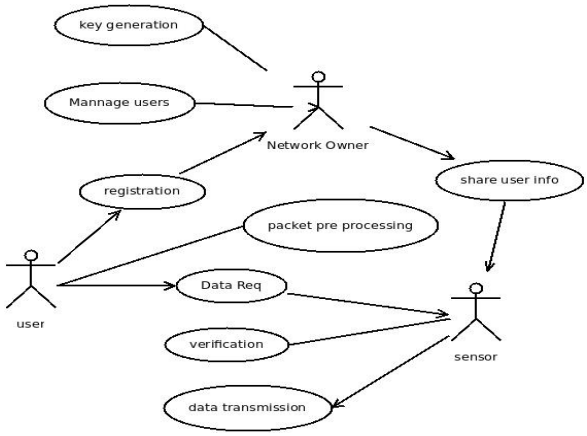


Fig.4 device interaction diagram

B. 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 $N \neq Nd_{Cricial}$
         1. $Ignore(Pkt)$
         2. $return$
      ii. $Switch_{neigh}(N \rightarrow Id_{Ex})$
      iii. $Move(N \rightarrow BS.pos)$

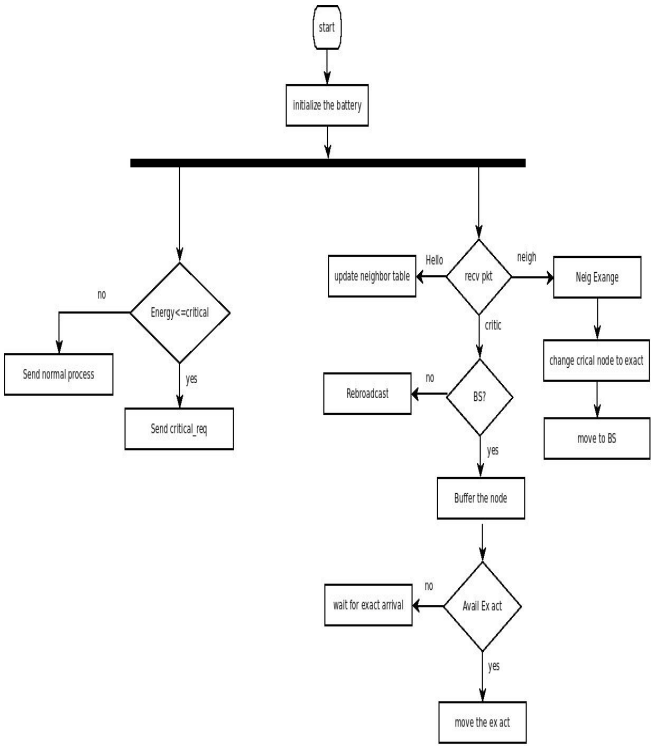


Fig.5 Failure rectifications

IV. RESULT

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

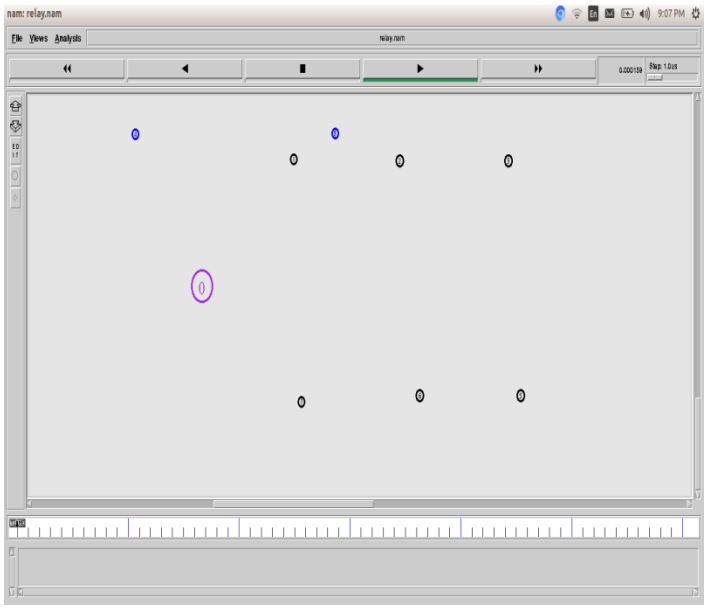


Fig.6 Network Placements

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

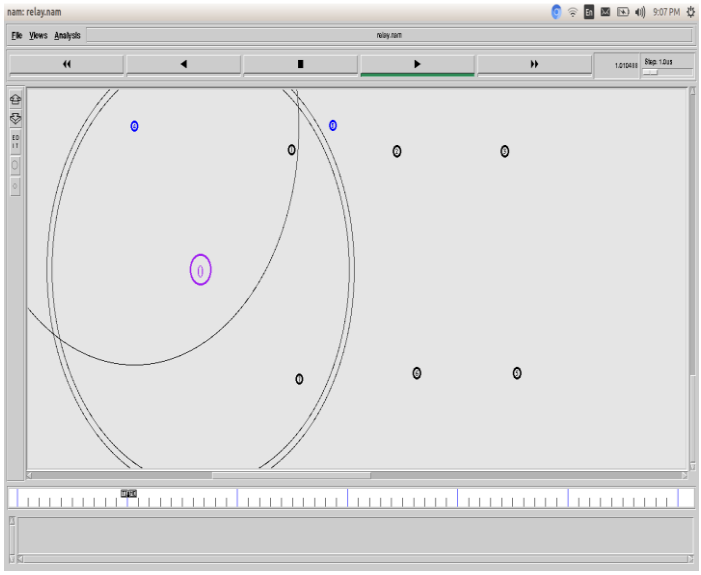


Fig.7 User registration process

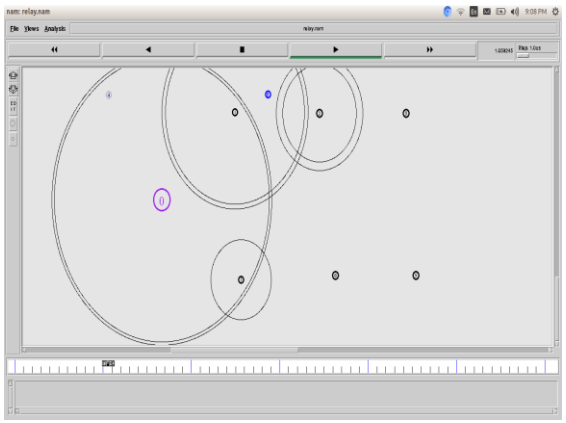


Fig.8 key sharing

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

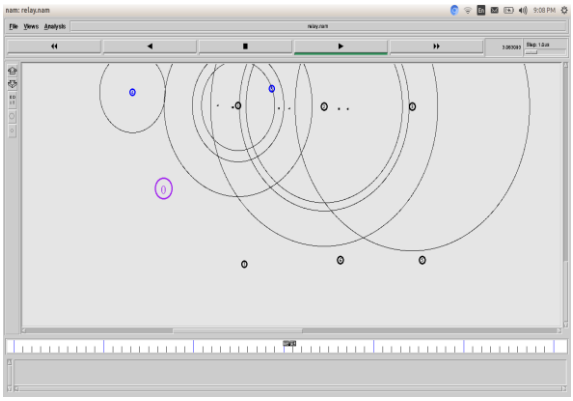


Fig.9 Secured Data transmission process

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)

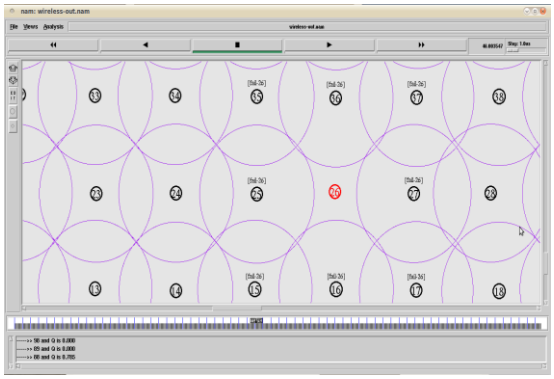


Fig.10 shows that the Failure detection and replacement system

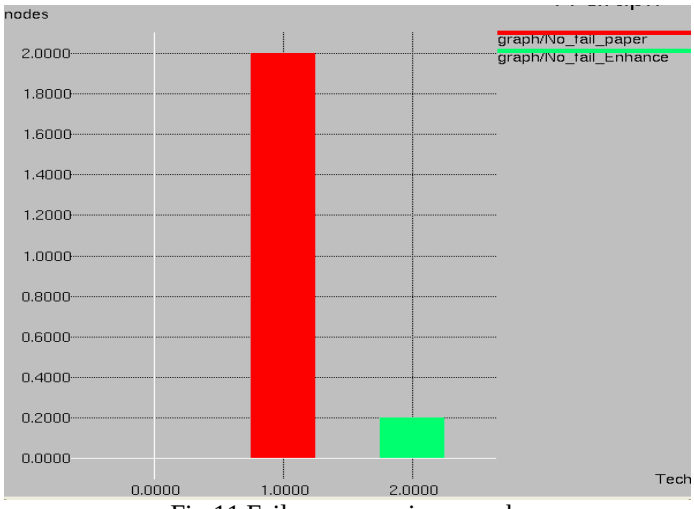


Fig.11 Failure comparison graph

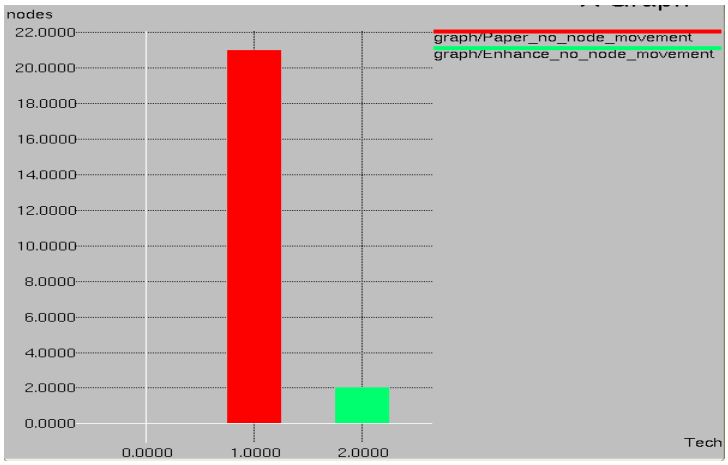


Fig.12. Node movement

V. CONCLUSION

In most of existing protocols author thought-about solely on the centralized knowledge dissemination strategies while not additional security and energy thought. we've projected the answer to determine the protection protocol which we have a tendency to extended the secured and distributed info delivery system with energy considerations. It's the primary distributed info discovery and dissemination protocol that allows network homeowners and approved users to disperse info things into WSNs while not relying on the bottom station and with network life time management. From our tested results, we are able to conclude that our analysis work providing sensible energy economical security design to wireless device network. In future, we'll autonomous device robotic network to boost the disaster management system.

VI. 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.

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

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

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

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

Alekhya K, pursued my post graduation in Master of Computer Applications from JTNU, Hyderabad, India, in 2011 and pursued my Bachelor degree in Computer Science from Osmania University, Hyderabad, India, in 2008. I have one year of teaching experience in computer science and also have one year experience in Software development. I'm very interested doing research in computer applications.