International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 5, May 2017 **ISSN 2319 - 4847**

HOP TO HOP CONFIDENTIALITY WITH DATA ENCODING IN WIRELESS SENSOR NETWORK

Jayshri B. Patil[1], G.R.Shinde[2]

[1]Department Of Computer Engineering, STES's SKNCOE Pune

[2]Department Of Computer Engineering, STES's SKNCOE Pune

ABSTRACT

In wireless sensor network messages are transferred between multiple source and destination pairs cooperatively such way that multi hop packet transmission is used. These data packets are transferred from intermediate node to sink node by forwarding packet to destination nodes. Where every node over hear transmission near neighbour node. To avoid this we propose novel approach with efficient routing protocol i.e. shortest path routing and distributed node routing algorithm. Proposed work also focuses on Automatic Repeat Request and Deterministic Network coding. We propagate this work by end to end message encoding mechanism. To enhance node security pairwise key generation is used, in which paired communicating node is assigned with pair key to make secure communication. End to end. We analyze both single and multiple nodes and compare simple ARQ and deterministic network coding as methods of transmission.

Keywords: Routing, wireless sensor network, UDP, Hop to Hop to communication.

1. INTRODUCTION

In multi hop wireless network packet transmission by preserving confidentiality of intermediate nodes, so that data sent to a node is not shared by any other node. Also in which confidentiality is not necessary, it may be not secure to consider that nodes will always remain uncompromised. In wireless network nodes data confidential can be viewed as a security to avoid a compromised node from accessing information from other uncompromised nodes. In a multi hop network, as data packets are transferred, intermediate nodes get all or part of the data packet through directly transmission of network node via multihop network fashion, when transferring confidential messages. Proposed work refers efficient algorithms for confidential multiuser communication over multi hop wireless networks. The metric we use to measure the confidentiality is the mutual information leakage rate to the relay nodes, i.e., the equivocationrate. We require this rate to be a small with high probability and inflict this in the resource allocation problem via an additional constraint. we consider practical delay requirements for each user, which eliminates the possibility of encoding over an arbitrarily long block.

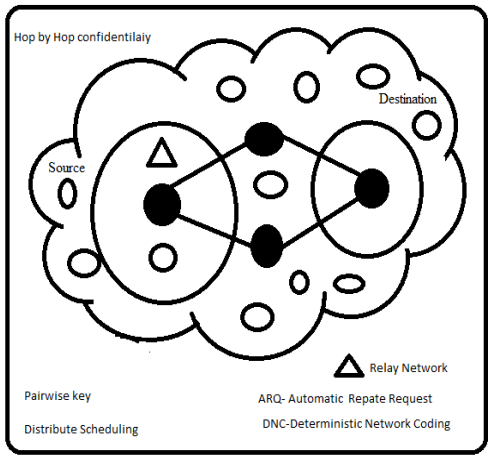
2. LITERATURE REVIEW

The paper presented by the YunusSarikaya, C. EmreKoksal April 2016 provides us with the details of how the resource allocation problem affect the network performance, confidentiality problem of intermediate node, dynamic control algorithm for a given encoding rate and we prove that our algorithm achieves utility arbitrarily close to the maximum achievable utility [1]. The paper presented by Tao Cui, TraceyHo, JörgKlieIr Jan 2013 gives the idea of Networks with unequal link capacities where a wiretapper can wiretap any subset of links, or networks where only a subset of links can be wiretapped. From this the Secrecy rate is achievable is determined. For the case of known but not unknown wiretap set as we know Determining the secrecy capacity is an NP-hard problem[2]. In the paper presented by AshishKhisti, Gregory W. WornellJuly 2010 proposed a masked beamforming scheme that radiates isotropically in all directions and show that it attains near-optimal performance in the high SNR regime. The secrecy capacity can be characterize in terms of generalized eigen values when the sender and eavesdropper have multiple antennas. The role of multiple antennas for secure communication is investigated within the framework of Wyner'swiretap channel.[3]. O. Ozan Koyluoglu, Can EmreKoksal, Hesham El Gamal May 2010. In this paper,the scaling behavior of the capacity of wireless networks under secrecy constraints and For extended networks with the path loss model is presented. A uniform rate per user is considered in this work. A path loss model is considered, where the legitimate and

eavesdropper nodes are assumed to be placed according to Poisson point processes with intensities.[4] The paper presented by N. Abuzainab and A. Ephremides Feb 2014, proposed scheme that Utilize private and public channels and wish to minimize the use of the (more expensive) private channel subject to a required level of security. Two transmissions schemes, a simple baseline ARQ scheme and the based on deterministic Network Coding can be considered for the proposed work.[5] Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor Mar 2010, In this paper, Use cooperating relays to improve the performance of secure wireless communications in the presence of one or more eavesdroppers. Three cooperative schemes have been considered: decode-and-forward, amplify-and-forward and cooperative jamming. Conclusion, Physical (PHY) layer security approaches for wireless communications can prevent eavesdropping without upper layer data encryption.[6]. C. Emre Koksal Feb 2013 presented that The secrecy constraint enforces an arbitrarily low mutual information leakage from the source to every node in the network, except for the sink node.In this paper, how private and open Information rate is achievable in regions of single- and multiuser wireless networks with node scheduling is studied[7]. Qizhong Yao. In this paper, author introduced the concept of delay-aware energy balancing this can be achieved with minimizing the average transmission delay and considering the issue of unbalanced harvested energy distribution. Every UE first harvests the RF energy emitted by the AP and then sends data to the AP directly or via other UEs acting as relays in a time multiplexing manner[8]. Abhijeet Bhorkar, IEEE 2015 Each packet transmission can be overheard by a random subset of receive nodes among which the next relay is selected opportunistic. The main aggravation in the design of minimum-delay routing policies is balance the trade-off between routing the and distribution the traffic[9]. Yi Gao. This paper presents Pathfinder, a robust path reconstruction method against packet losses as as routing dynamics. At the node side .In this paper Wireless Sensor Networks, 1. Measurement 2.Path Reconstruction methodology is given.[10]. Ahmed E.A.A. Abdulla July 2012. In this paper author proposed Hybrid Multi-hop routing (HYMN) algorithm, which is combination of two algorithms namely, flat multi hop routing. In this paper focus is given on Wireless sensor Networks, Energy hole problem, Sink node Isolation [11]. Sanghita Bhattacharyaa, SubhansuBandyopadhyayb 2012, In this paper author considered interference, transmission power and reception power of nodes asymetrics to derive a good quality routing path for delivering the packets from source to destination. For a given source to destination pair in the network, there may exist more than one routing paths. Selecting a low interference energy efficient routing path gives a good balance between the interference and energy utilization. Designed algorithm selects the low interference energy efficient path among all the paths for a given source destination node pair [12]. A. Eryilmaz, R. Srikant Apr 2015, Authors studied the problem of stable scheduling for a class of wireless networks. Their aim is that to equilibrium the queues holding information to be transmitted over a fading channel. In this case prove that, for any mean arrival rate which lies in the capacity region, the queues will be stable under designed stategy[13].C. Manikandan, S. BhashyamDec 2009, The downlink scheduling problem is considered. Two policies which make allocations based on predicted channel states are designed. The first is based on the well-known dynamic backpressure policy to the undetermined channel case. The second is a variant that improves delay performance under light loads.[14].

3. SYSTEM ARCHITECTURE

The following figure 1. Shows that how the communication is done between different wireless sensor networks. Proposed system manages overlapped wireless sensor network with following architecture. Proposed system implements an optimal dynamic policy for the case in which the number of blocks across which secrecy encoding is performed is asymptotically large Next to that, This work propagate encoding between a finite number of data packets, which removes the possibility of achieving perfect secrecy. In this case, proposed work design a dynamic policy to select the encoding rates for every data packet, based on the instantaneous channel state information, queue states and secrecy humiliation requirements. By numerical analysis, we observe that the proposed design resembles the optimal rates asymptotically with increasing block size. Finally, we address the impact of practical implementation issues such as infrequent queue updates and de-centralized scheduling of nodes. Existing work present the efficiency of our policies by numerical studies under various network conditions. Next to this work proposed system contribute for deterministic network coding Automation of repeat packet request mechanism to actively transfer data packet. This help to network costs and other system parameters were just designed as constants in our work the network costs are related to physical layer parameters such as channel encoding parameters and transmission power. Here proposed system design in the way, which formulate problem by adding noise to original message or request at destination. Proposed system also formulate problem ARQ case in which automatic repeat request is send between numbers of time slot during packet sending. Where, packets are generally transferred via private channel and public channel from source to destination. These packets are generally geometrically distributed among network nodes.Proposed work focus work to achieve node confidentiality need to encode block of information across multiple packet. Where, adaptive end to end to encoding scheme is applied for node confidentiality.



- Cooperation between sensor WSN**:-** It is assumed that a WSN has a rational and selfish character and will only cooperate with another network if this association provides services that justify the cooperation.
- Reduce Delay:-The delay need to reduce in multipath routing because backup routes are identified during route discovery.
- Load Balancing**:-**traffic distribution is not equal in all links in the network, spreading the traffic along multiple routes can reduce congestion in some links and bottlenecks.
- Increase lifetime of WSN:-The original idea behind using multipath routing approach in WSN was to provide path resilience and data transmission reliably. In the fault tolerance domain, whenever a sensor node does not send its data packets towards the sink node, it can benefit from the availability of alternative paths to transfer its data packets from node or link failures.
- Maximize the success ratio:-Active routing scheme need to design for maximizing success ratio.

4. MATHEMATICAL MODEL

- End-to-end Encoding: At every generation of new confidential message, i.e., Let , $P_s(t)=0$, let $k_s(t+1)=k_s(t)+1$,and determine end-to-end confidential encoding rate.
- Flow control: At each block, for some, each source injects confidential bits into its queues
- Encoding:-Encoding of each letter in secret message by its equivalent ASCII code
  1. Conversion of ASCII code to equivalent 8 bit binary number.
  2. Division of 8 bit binary number into two 4 bit parts.
  3. Choose of suitable letters corresponding to the 4 bit parts.
  4. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
  5. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
  6. Encoding is not case sensitive.
- Decoding
  1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.
  2. 4 bit binary numbers of combined to obtain 8 bit number.
  3. ASCII codes are obtained from 8 bit numbers.
  4. Finally, secret message is recovered from ASCII codes.

Let us consider S as a set confidential Wireless Sensor Networks with effective key management…
S= { }
INPUT: Identify the inputs as number of nodes
F= {f_1, f_2, f_3 ....., f_n| 'F' as set of functions to execute to routing model}
I= {i_1, i_2, i_3…|'I' sets of inputs to number of nodes/ sensors}
O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}
S= {I, F, O}
I = {Number of nodes}
O = {Shortest routing path for multi hop protocol}
F = {AODV, ARQ,, Euclidean distance, Pair wise key}

5.SYSTEM ANALYSIS

5.1. Performance Measures

a) Throughput Maximization:-Throughput maximization is achieved by reducing delay ratio and improving packet delivery ratio in WSN

b) Packet Delivery Ratio:- This measure is used for average packet delivery ratio to verify WSN communication. Packet transmission needs to send packet energy efficient which result in maximizing throughput.

c) Routing Over Head (ROH):- In wireless sensor network packet is sending performed by moving sensor nodes using hop to hop, Due to that overhead cost increased. Proposed network decreased overhead by shortest path communication.

d) Average End to End Delay (ms) :- Average end to end delay ratio reduced by queue management for efficient network communication.

5.2. Result Analysis

In this section performance metrics are used to evaluate performance of routing protocols and data dissemination protocols scheme when no in networking processing is performed and no caching is used.

Simulation Parameter:

Table No.1 Simulation Parameter

Parameter	**Value**
Simulation Time	500ms
Terrain Area	600*500
Time Arrival	32ms
Protocol	DSR
No of Node	25,45,100

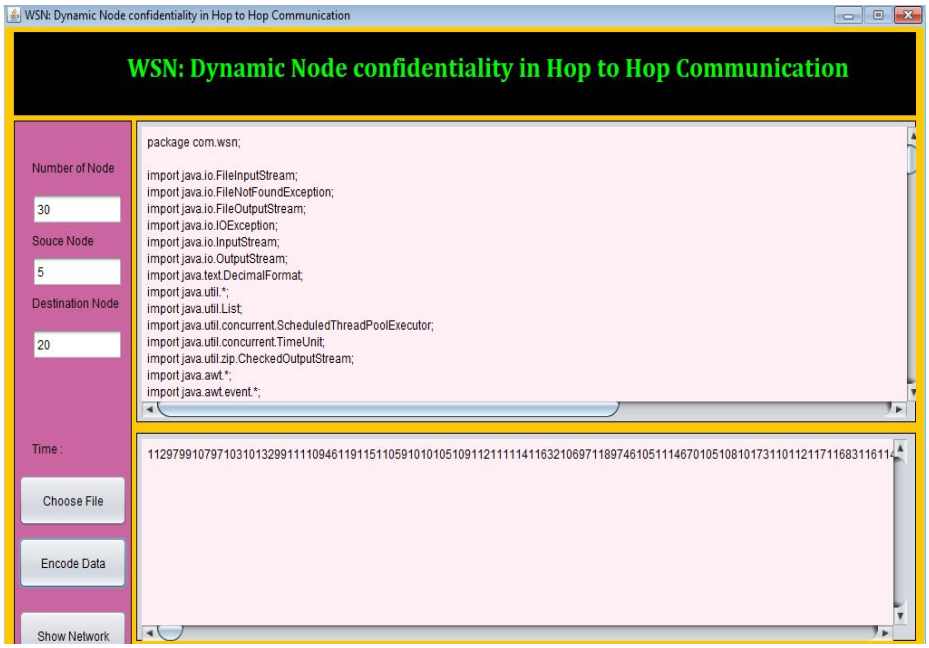


Fig. 2 File Encoding

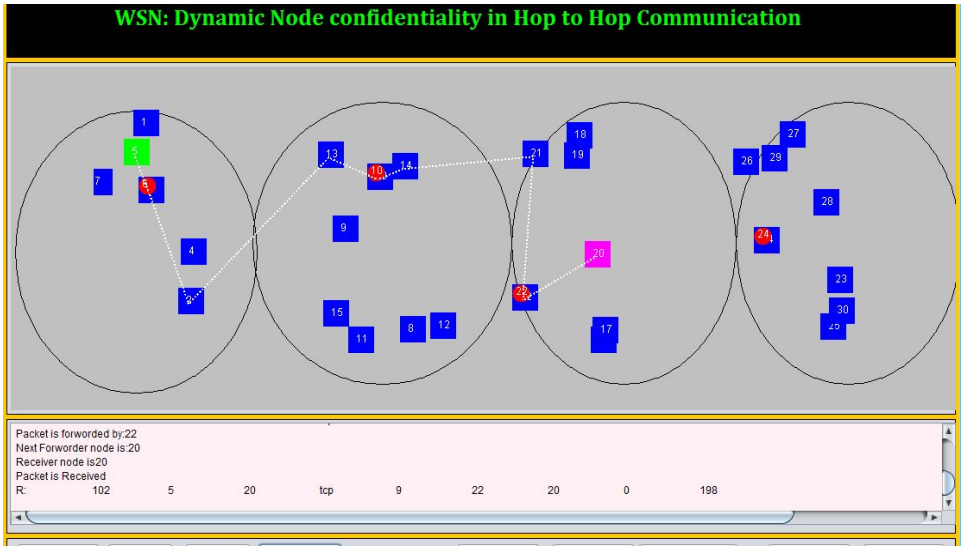


Fig.3 Network Formation

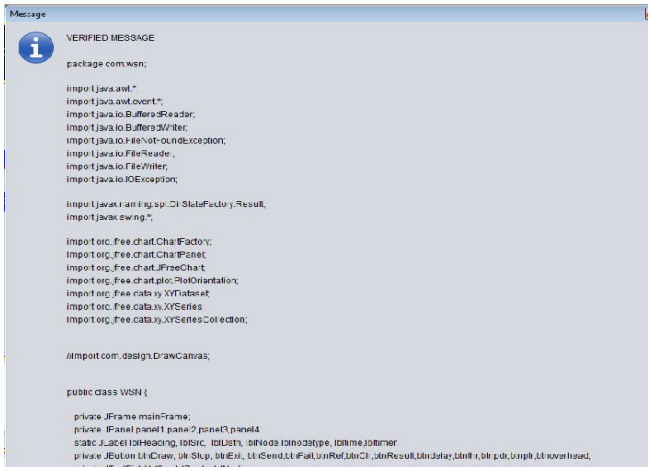


Fig.4 File Verification

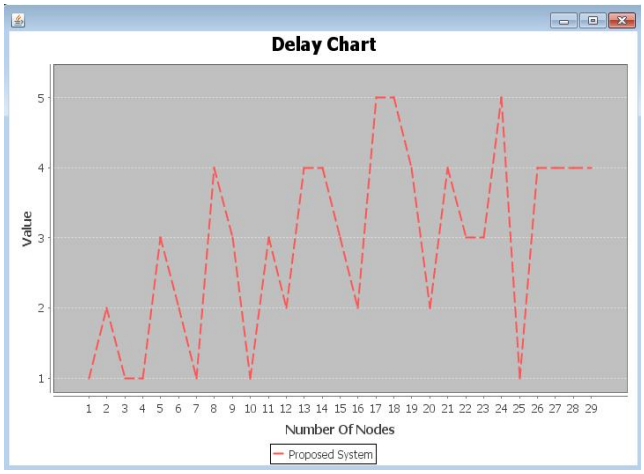


Fig.5 Delay Chart

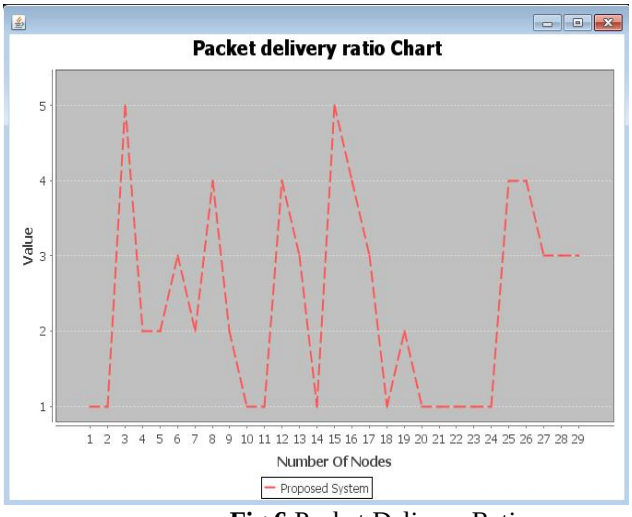


Fig.6 Packet Delivery Ratio

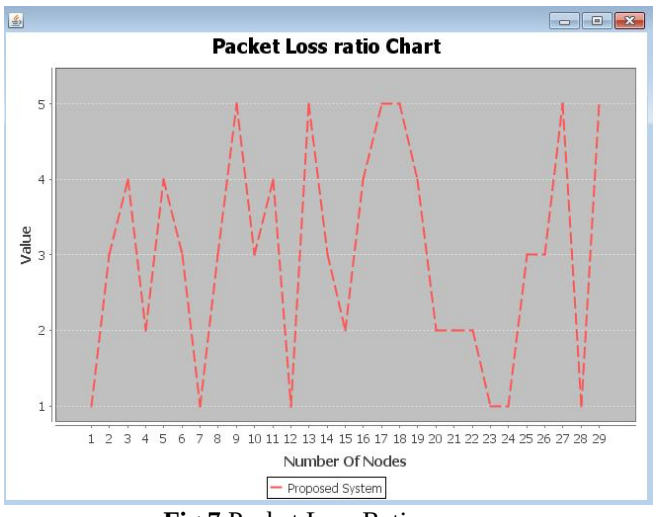


Fig.7 Packet Loss Ratio

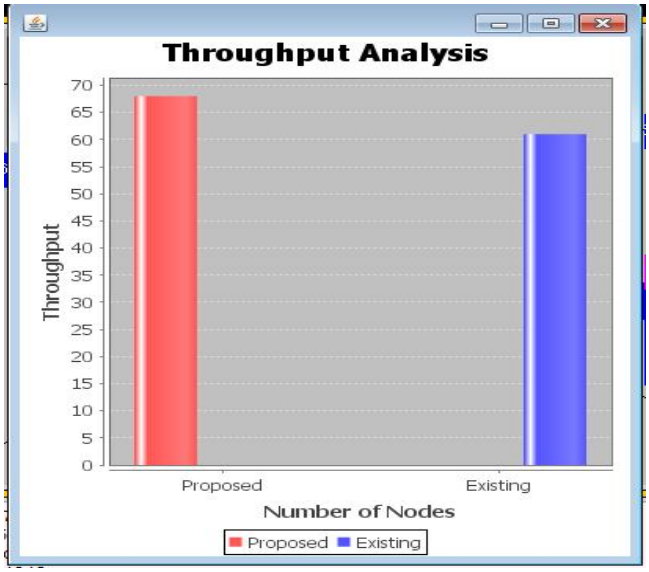


Fig.8 Throughput Analysis

Table No.2 Comparison of proposed and existing system

Goals	Existing System%	Proposed System%
Throughput	80	90
Network	Unicast- Hop by Hop	Mesh based multi antenna-Multicast Network
Controller	KGC	Base Station Controller
Security	Certified Security	Node confidentiality with secret key
Protocol	DSR	Radio Resource Control

Proposed system is expected to maximize throughput for node to node confidentially in packet transmission n wireless sensor network. To achieve sensor node security in wireless network this system used noise aided packet transmission. Proposed system designed for multi antenna for multicast wireless network.
Proposed system designed to implement following :

-Network Formation and clustered Communication
-Mesh Network Formation
-Multi antenna based routing
-Throughput Maximization.

6.CONCLUSION

In this we implemented Secure and efficient path reconstruction for packet losses as well as routing . At the node side, Pathfinder is mechanism routs and efficiently manages the path information using path difference. Simple Automatic Repeat Request (ARQ), and Deterministic Network Coding (DNC), where in each time slot the source forms M linearly independent deterministic combinations of the M packets and then use simple ARQ to transmit each linear combination reliably to the destination. We assume in this case that the receiver does not make any changes from the received linear combinations but either decodes the transmitted packets or not. Security key are used for in sensor nodes authentication and authorization in wireless network for packet transfer. Dynamic sensor network uses sensor

deployment for improving network lifetime. Here in this network density monitored area to determine optimal sensor deployment.

References

[1] YunusSarikaya, C. EmreKoksal, Senior Member, IEEE, and OzgurErcetin, " Dynamic Network Control for ConfidentialMulti-Hop Communications" , IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 24, NO. 2, APRIL 2016.

[2] T. Cui, T. Ho, and J. KlieIr, "On secure network coding with nonuniform or restricted wiretap sets," IEEE Trans. Inf. Theory, vol. 59, no. 1, pp.166–176, Jan. 2013.

[3] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas:Themisome wiretap channel," IEEE Trans. Inf. Theory, vol.56, no. 7, pp. 3088–3014, July 2010.

[4] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," IEEE Trans. Inf. Theory, vol. 58, no. 5, pp. 3000–3015, May 2012.

[5] N. Abuzainab and A. Ephremides, "Secure distributed information exchange," IEEE Trans. Inf. Theory, vol. 60, no. 2, pp. 1126–1135, Feb. 2014.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 4033–4039, Mar. 2010.

[7] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," IEEE/ACM Trans. Netw., vol. 21, no. 1, pp. 324–337, Feb. 2013.

[8]C. EmreKoksal "Control of Wireless Networks With Secrecy" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 1,FEBRUARY 2013.

[9] AbhijeetBhorkar "Opportunistic Routing With Congestion Diversity in Wireless Ad Hoc Networks" IEEE/ACM TRANSACTIONS ON NETWORKING1063-6692 © 2015 IEEE.

[10]Yi Gao "Towards Reconstructing Routing Paths in Large Scale Sensor Networks" 10.1109/TC.2015.2417564, IEEE Transactions on Computers.

[11] Ahmed E.A.A. Abdulla "HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 7, JULY 2012.

[12] SanghitaBhattacharyaa, SubhansuBandyopadhyayb, "An Interference Aware Minimum Energy Routing Protocol forWireless Networks Considering Transmission and ReceptionPower of Nodes", Procedia Technology 4 (2012) 1 – 8, 2212-0173,C3IT-2012.

[13] A. Eryilmaz, R. Srikant, and J. R. Perkins, "Stable scheduling policiesfor fading wireless channels," IEEE Trans. Inf. Theory, vol. 13, no. 2,pp.411–424, Apr. 2005.

[14] C. Manikandan, S. Bhashyam, and R. Sundaresan, "Cross-layer schedulingwith infrequent channel and queue measurements," IEEE Trans.Wireless Commun., vol. 8, no. 12, pp. 5737–5742, Dec. 2009.