www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16589-16594

GALSR: Geographical Based Adaptive Lifetime Secure Routing Protocol For Wireless Sensor Network

Hanan Raj.R[1], Shanthameena.C[2]

Research Scholar, Department of computer science and Engineering, A.R.J college of Engineering,Mannargudi, India [1]
Assistant professor, Department of computer science and Engineering, A.R.J college of Engineering,Mannargudi, India

Abstract: ***Wireless sensor networks (WSNs) are potentially increased in research field due to their wide range of application. The topology of advanced WSNs form Multi-Hop WSNs. The Main issues in this topology is location based security and lifetime preserving in energy resources. In this paper, we projected a Geographical based Adaptive Lifetime Security Routing (GALSR) Protocol and GALSR Algorithm to improve the lifetime and security of WSNs. This algorithm enhanced with Greedy for Shortest path finder and Direct Random Propagation for Random Walking. We then determine that the energy consumption is rigorously disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To resolve this issue, we introduce non-uniform energy deployment to optimize the lifetime and message delivery ratio under same energy resources and security. This energy balancing is set by Energy balance control (EBC) and security parameter using Metric Energy Balancer (MEB).We validate our finding in both Quantitative and Qualitative measures. Our quantitative measures is shown out of NetSim Simulator similarly our implementation is an best prove for our qualitative measures, Our proposed model shows that we achieved with increased Lifetime, Adaptive Security and Monetary efficient protocol.***

Keywords: Multi-hop Wireless Sensor Network, Geographical based Adaptive Lifetime Security Routing, Energy Balance Control, and Metric Energy Balancer.

1. Introduction

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN) are spatially spreaded independent sensors to observer physical or environmental conditions, such as temperature, sound, pressure, etc. and to supportively permit their data over the network to a main location. The added contemporary networks are bi-directional, also assisting governor of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield investigation; nowadays such networks are used in many industrial and applications, such as process monitoring and control, machine monitoring, and so on.The WSN is made of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Such sensor network node has numerous parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit meant for interfacing with the sensors and an energy source, generally a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the mass of a grain of dust, though functioning "iota" of authentic microscopic scales have yet to be created. The sensor nodes cost is similarly inconstant, ranging from a few to hundreds of rupees, depending on the complexity of the individual sensor nodes. Cost and Size constraints on sensor nodes effect in corresponding constraints on resources such as energy, memory, communications bandwidth and computational speed. The topology of the WSNs can vary from a meek star network to an advanced multi-hop wireless mesh network. The propagation method among the hops of the network can be flooding or routing. Wireless sensor networks (WSNs) are enticing growing research attention, due to their widespread spectrum of applications, counting military purposes for monitoring, tracking and surveillance of borders, intelligent transportation systems for monitoring road conditions and traffic density, and environmental applications to monitor, for example, atmospheric pollution, water quality, agriculture, etc. AWSN is composed of a number of sensor nodes (SN) transmitting wirelessly the information they capture. An SN is generally composed of a power unit, Sensing unit, communication unit and processing unit. Power consumption, Security and Lifetime is the main limiting factor of an SN. In point, SNs are in common requisite to operate freely and independently for a huge phase of time in areas where power infrastructure may not be presented. The wireless communication unit can also guarantee a mechanism for ad-hoc communication between SNs forming a WSN.

In fact, in some scenarios, it might be more energy efficient to transmit a message via multi-hop communications over short distances instead of a single hop long distance transmission to the base station (BS).Motivated by this fact that WSNs routing is often geography based, we propose a GALSR : Geographical based Adaptive Lifetime Secure Routing Protocol for Wireless Sensor Network without traceback attack and packet loss and energy loss. The balanced energy monitorance is accomplishing using Metric Energy Balancer. For the non-uniform energy deployment, our analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than the existing measure. In count, we also stretch quantitative secure analysis on the proposed routing protocol based on the criteria proposed in [1].GALSR protocol has two major advantages: (i) It guarantees balanced energy consumption of the intact sensor network so That the lifetime of the WSNs can be maximized. (ii) GALSR Protocol

supports multiple routing strategies based on the routing requirements, together with fast/slow message delivery and secure message delivery to avert malicious traffic jamming attacks and routing trace back attacks in WSNs

2. RELATED WORK

Yun li and et al implements Wireless sensor networks (WSNs) have been widely used in many areas for critical infrastructure monitoring and information collection. While privacy of the message can be guaranteed through content encryption, it is much more difficult to adequately address source-location privacy (SLP).For WSNs, SLP service is extra byzantine by the nature that the sensor nodes generally consist of low-cost and low-power radio devices. The intensive cryptographic algorithms (such as public-key cryptosystems), and broadcasting-based protocols may not be suitable. In this paper, we first suggest standards to quantitatively measure source-location information leakage in routing-based SLP protection schemes for WSNs. Through this model, we recognize vulnerabilities of some well-known SLP protection schemes.

We then recommend a system to provide SLP through routing to a randomly selected intermediate node (RSIN) and a network mixing ring (NMR). Our security investigation, based on the planned criteria, displays that the proposed scheme can deliver excellent SLP. The ample simulation results demonstrate that the proposed scheme is very effectual and can attain a high message delivery ratio. We trust it can be used in numerous practical applications. Lifetime is extra area that has been widely studied in WSNs R.Govindan and et al proposed, This paper addresses query based geographic and energy aware routing (GEAR) In GEAR, the sink node distribute requests with geographic attributes to the target region as an alternative of using flooding.Based on learning cost and estimated cost, each node forwards messages to its neighboring nodes. The estimated cost reflects both the distance to the destination and the outstanding energy of the nodes. Where the local minimum problem is occurs due to carriage of learning cost.

While geographic routing algorithms have the returns that each node only desires to keep its neighboring information, and delivers a higher efficiency and an improved reachable for large scale WSNs, the algorithms may grasp their local minimum, which can outcome in dead end or loops. To unravel the local minimum problem, some variations of these simple routing algorithms were proposed. Jian work a Message authentication is one of the most actual ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this determination, many message validation systems have been established, constructed on either symmetric-key cryptosystems or public-key cryptosystems. Furthermost of them, however, have the limitations of high computational and communication directly above in addition to dearth of scalability and resilience to node compromise attacks. To account these problems, a polynomial-centered scheme was recently presented. However, this scheme and its extensions all have the faintness of a built-in threshold resolute by the degree of the polynomial: when the number of messages conveyed is greater than this threshold, the adversary can fully recuperate the polynomial. In this paper, it deal authentication plan based on elliptic curve cryptography.

While allotting intermediate nodes authentication, our planned scheme allows any node to conduct a limitless number of messages without suffering the threshold problem. In accumulation, our scheme can also deliver message source discretion. Both theoretical analysis and simulation outcomes determine that our proposed scheme is extra effective than the polynomial- centered method in expressions of computational and communication overhead below comparable security stages while offering message source privacy.

3. MODEL AND ASSUMPTION

3.1 System Model

The objective is to improve the lifetime and security of WSNs. This algorithm enhanced with Greedy for Shortest path finder and Direct Random Propagation for Random Walking. We then find that the energy consumption is brutally disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To resolve this issue, we introduce non-uniform energy deployment to optimize the lifetime and message delivery ratio under same energy resources and security. This energy balancing is set by Energy balance control (EBC) and security parameter using Metric Energy Balancer (MEB)

3.2 Design Goals

1)We propose a GALSR: Geographical Based Adaptive Lifetime Secure Routing Protocol for Wireless Sensor Network for WSNs. In this protocol, Geography based routing strategies can be applied to address the message delivery requirements.2) We design the advanced schema to provide balanced Energy consumption to maximize the lifetime and message delivery under the same energy deployment.3) We develop theoretical formulas to estimate the number of routing hops in GALSR under varying routing energy Balance control and security requirements.4) We quantitatively analyze security of the projected routing algorithm.5) Our theoretical and simulation results both show that under the same total energy deployment, we can growth the lifetime and the number of messages that can be brought more than four times in the non-uniform energy deployment scenario.

3.3 Overview of Proposed System

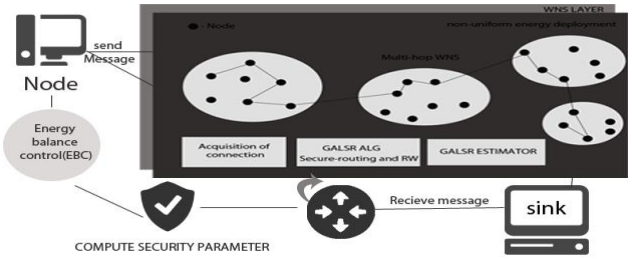

Fig 1 System Architecture

In above fig 1 Network is shaped for secure routing. It network is consistently divided into small grids. Energy Balance Routing lead message from sensor to sink using EBC (Energy Balance Control) parameter $\alpha \in [0, 1]$ Node upholds its relative location and the remaining energy levels of its immediate adjacent neighboring grid. Calculates the security parameter β for secure routing using cost factor f. This security

DOI: 10.18535/ijecs/v5i5.43

parameter β is used to discovery the maximum routing security level. The routing protocol contains two choices for message forwarding 1. Regulates shortest path routing 2. Random walking. Choose anyone of routing to reach the sink node.

4. The proposed GALSR routing protocol

we now explain the proposed GALSR protocol based on the protocol using dissimilar routing to grasp the destination. In this paper emphasis on the shortest path routing and random walking and also balance the energy consumption.

4.1 Network formation

In this module the network is formed for secure routing. The networks are constituted of a large number of sensor nodes and a sink node. Each sensor node has an exact limited and non-replenishable energy resource. The sink node is the solitary destination for all sensor nodes to send messages to via multi-hop routing strategy.

The network is consistently divided into small grids. Each grid has a relative location founded on the grid information. The node in every grid with the highest energy level is designated as the head node for message forwarding.

Each node in the grid will maintain its own attributes, including location information, end during energy level of its grid, as well as the attributes of its adjacent neighboring grids. The information preserved by every sensor node will be updated periodically.

4.2 Energy Balancing Routing

This module send message from sensor to sink by means of EBC (Energy Balance Control) parameter $\alpha \in [0, 1]$.

Node upholds its relative location and the remaining energy levels of its immediate adjacent neighboring grids. For node A, specify the set of its immediate adjacent neighboring grids as N_A and the remaining energy of grid i as Er_i , $i \in N_A$. With this information, the node A can calculate the average remaining energy of the grids in N_A as $E_a(A) = 1/N_A \sum i \in N_A Er_{i..}$

To attain energy balance between all the grids in the sensor network Metric Energy Balancer is involved, we carefully monitor and control the energy consumption for the nodes with relatively low energy levels by configuring *A* to only select the grids with comparatively higher remaining energy levels for message forwarding.

The candidate set for the following hop node as $N^{\alpha}_A = \{i \in N_A \mid Er_i \geq \alpha E_a(A)\}$ assembled on the EBC α. Increasing of a value may also upturn the routing length. However, it can effectually control energy consumption from the nodes with energy levels lower than αEa(A).

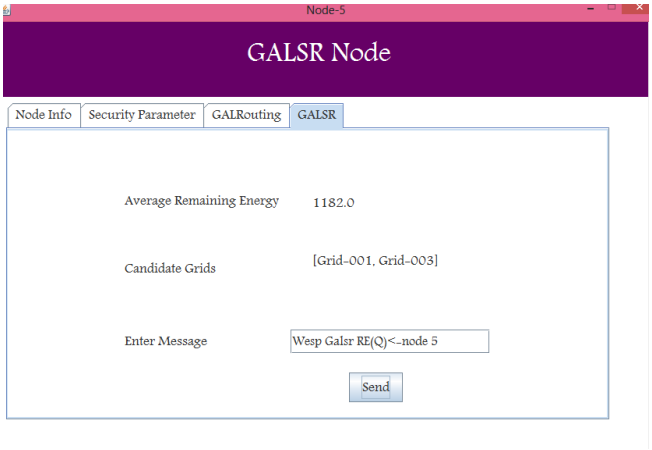

Fig 3 GALSR Node

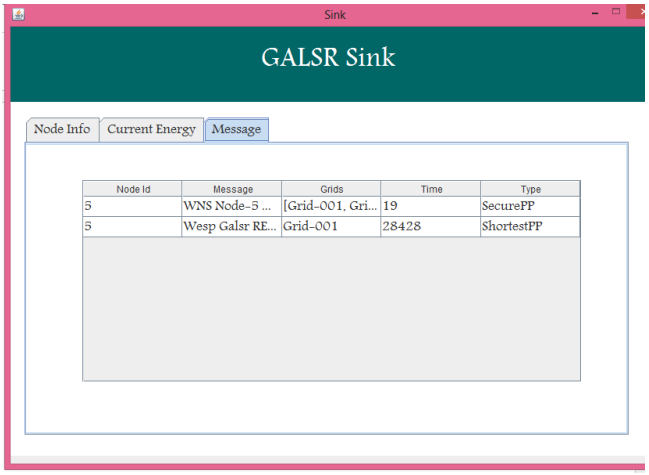

Fig 3 GALSR Node & sink

4.3 Secure Parameter Computing

This module calculates security parameter β for secure routing by cost factor f. This security parameter β is used to discover the maximum routing security level. In table 1 show some computational value.

The following steps are used to calculate β

1. $a \leftarrow 4f^2; c \leftarrow -5; e \leftarrow -1;$
2. $A \leftarrow \frac{c}{a}; B \leftarrow \frac{d}{a}; C \leftarrow \frac{e}{a};$
3. $p \leftarrow -\frac{1}{12}A^2 - C; q \leftarrow -\frac{A^3}{108} + \frac{AC}{3} - \frac{B^2}{8};$
4. $r \leftarrow -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}};$
5. $u \leftarrow \sqrt[3]{r};$
6. $y \leftarrow -\frac{5}{6}A + u - \frac{p}{3u}; w \leftarrow \sqrt{A + 2y};$
7. $s \leftarrow \frac{-w + \sqrt{-3A + 2y + 2B/w}}{2};$
8. $\beta \leftarrow 1 - s$

Table1

(Secure Parameter Computation)

S,NO	COSTFACTOR	BETA VALUE
1	3	0.565
2	20	0.836
3	1	0.009

4.4 GALSR Routing

It delivers routing path security and unpredictability. The routing protocol comprises two options for message forwarding: Shortest path and Random walking.

Algorithm:

Input: Calculate the average remaining energy of the adjacent neighboring grids:

$$\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$$

1. Decide the candidate grids for the consequent routing hop :
$$\mathcal{N}_A^{\alpha} = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$$
2. Select the random number α [0,1]
3. If $\alpha > \beta$ then
4. Direct the message to the grid in the N^{α}_A that is closest to the sink node grounded on relative location
5. Else
6. Path the message to a random selected grid in set N^{α}_A
7. end if

In the deterministic routing approach, the following hop grid is nominated from N^{α}_A based on the relative locations of the grids. The grid that is nearby to the sink node is selected for message forwarding. In the secure routing case, the following hop grid is arbitrarily selected from N^{α}_A for message forwarding. The distribution of these two algorithms is structured by a security level called $\beta \in [0, 1]$ carried in each message. To forward the message node select the random number $\gamma \in [0,1]$, when $\gamma > \beta$ then the node selects the next hop grid grounded on the shortest routing algorithm; otherwise, the next hop grid is selected using random walking. β is an adjustable parameter set as security level. The more energy effiency in messaging is obtain when the β value is small.

4.5 GALSR Estimator

Develop theoretical formulas to estimate the number of routing hops in GALSR under varying routing energy balance control (EBC) and security requirements. A quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are raised under the same energy deployment(ED). We develop the quantitative measure to standardize our GALSR protocol.

5. DETERMINE SECURITY LEVEL BASED ON SECURITY PARAMETER COMPUTATION

` For node A, denote the set of its immediate adjacent grids as N_A and the remaining energy of grid i as Er_i , $i \in N_A$. With this information, the node A can compute the average remaining energy of the grids in N_A as $E_a(A) = 1/N_A \sum i \in N_A Er_{i..}$

Where metric energy balancer assured with ME

ME with I as i=(1,2,3,4)the energy distribution level is varied upon the distribution factor as such

Me=PE($\in (F)^2$) where p(4. $\in$<0),i=1..4

Where set probabilistically hop distance set through p,q,r,u,and y

h be the hob estimated, Nm node

Nm=0 i=1; s=0 i=2;

The Set of value is adjacent node is determined by the x factor and set with the value of x w and $a^{n.}$

$$P(zi) = \sum_{j=0}^{4} \binom{n}{Me} x^w a^{n-k}$$

x=h(1/4f^2) and For each layer, the energy consumption for sensing and forwarding also follow the nor-mal distribution.

P(zi)=4f where node i=1,2,3,4. Where a is

The network is randomly deployed and every sensor node is initially deployed with equivalent initial energy. We also don that data generation in each sensor node is a random variable. Then for a specified routing cost factor f, the optimal security level can be calculate approximately Calculated.

5.1 Security Analysis

GALSR provide the secure routing using GALSR Algorithm**.**

The Proposed GALSR Protocol achieve a high message delivery ratio and the total number of message delivered is 4.2 times higher than existing protocol for the non-uniform energy deployment, It Prevent from routing traceback attacks.

6. PERFORMANCE EVALUATION AND SIMULATION RESULT

The Quantitative measure of our model is evidence by using NetSim. The Uniform Energy Deployment and non-uniform energy deployment is compared. Different energy level is deployed for every node. From the simulation that the delivery ratio increases with a. Evaluating to uniform energy deployment, the delivery ratio used for non-uniform energy deployment is much higher than the uniform energy deployment with the same a. We also equated the total number of messages that can be delivered in the two scenarios. The Message delivery ratio is resulted about 95%.In uniform energy deployment, the number of messages that can be delivered is 1,510 and in Non-Uniform energy deployment the number of messages that can be delivered increases to 1,624. The EBC Metric determine the calculative measures of GALSR node

And its Sink deterministic energy deployment in respect to security constrain, Total Message delivery rate and Energy deploy mentation. The Simulated Result shows the Actual performance of our network. Fig 3 explain the message count delivery rate with respect to the node /sink receiver and Time count. Fig 3 describe the balanced energy distribution of different node, Fig 4 provide the Security parameter with respect to calculated Formulae.

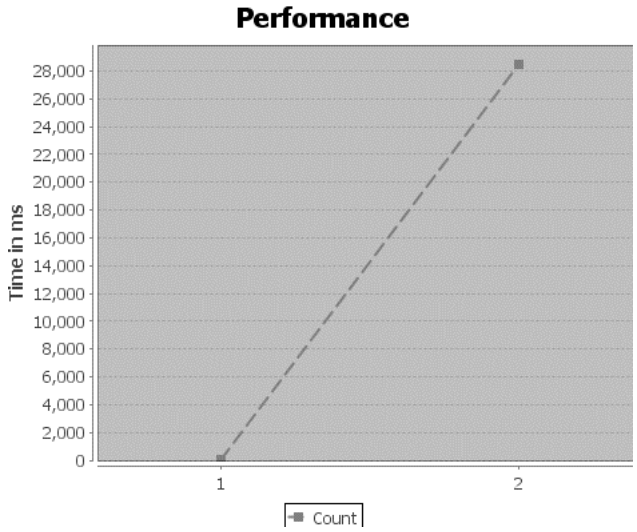

Fig 4 Perfomance Analysis on Message Count Delivery Rate

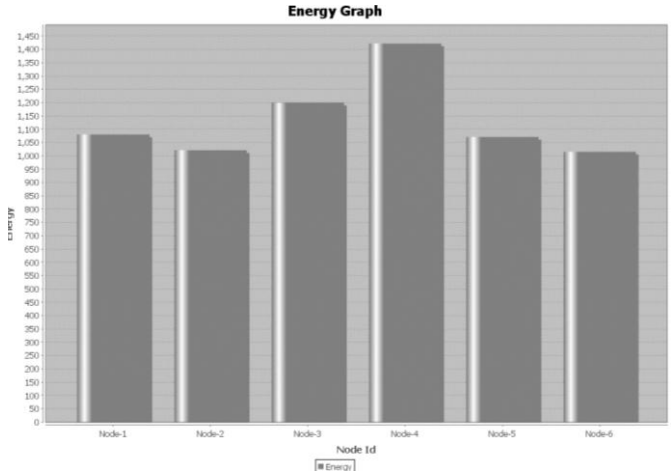

Fig 5 Performance Ananlysis on Balanced Energy on Non-Uniform Deploymentation

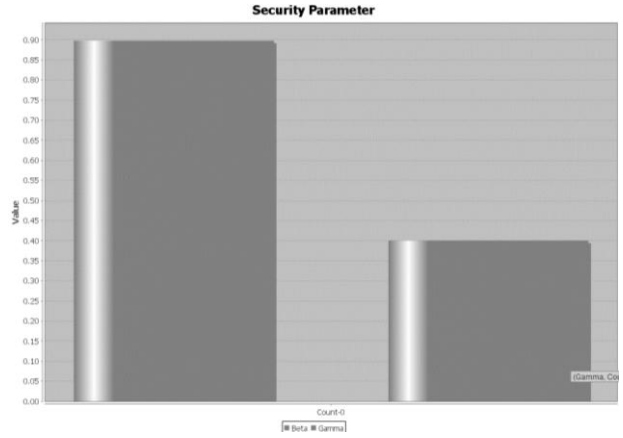

Fig 6 Performance Analysis on Security Parameter using GALSR

7. CONCLUSION

We executed the adaptive mode to improve the Lifetime and increased Message Delivery of Wireless Sensor Network. The Protocol is designed for both uniform energy Deployment and Non-Uniform Energy Deployment. The model provide the elasticity to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both the Experimental and Analytical measures that GALSR has an exceptional routing implementation in terms of energy balance and routing path allocation for routing path security. We achieved 4.2 times higher rate of resultant in terms of GALSR Protocol.

REFERENCES

[1] Di Tang,Tongtong Li,Jian Ren. (2015), "Cost Aware Secure Routing Protocol Design for Wireless Sensor Protocol," in IEEE Transaction on Parallel and Distributed Systems, Vol 26, No 4, April 2015.

[2] Bulusu N, Heidemann J., and Estrin D. (2000)., "GPS-less low cost out- door localization for very small devices," Comput. Sci. Dept., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729

[3] Bose P., Morin P., Stojmenovic I., and. Urrutia J. (1999), "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., pp. 48–55.

[4] Bose P, Morin P., Stojmenovic I., and Urrutia J.(1999), "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd ACM Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., Seattle, WA, USA, pp. 48–55.

[5] Estrin D , Heidemann J. and Xu Y.(2001), "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., , pp. 70–84..

[6] Karp B. and Kung H. T. (2000), "GPSR: Greedy perimeter stateless rout- ing for wireless networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, pp. 243–254

[7] Li J. and Jannotti J. and De Couto D. S. J. and Karger D. R. and Morris R.(2000) , "A scalable location service for geographic ad hoc routing," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw, pp. 120–130.

[8]. Li Y. and Ren J. and Wu J. (2012), "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, No. 7, pp. 1302–1311.

[9] Li Y., Yang Y., and Lu X.(2010), "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582.

[10] Li Y. and Ren J. and Wu J.(2012), "Providing hop-by-hop authentica- tion and source privacy in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, pp. 3071–3075.

[11]. Melodia T., Pompili D., and Akyildiz I.(2004), "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in Proc. IEEE Conf. Comput. Commun., Mar., vol. 3, pp. 1705–1716.

[12] Savvides A., Han C.-C., and. Srivastava M. B.(2001), "Dynamic fine- grained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., . pp. 166-179

[13] Yu Y. and Govindan R. and Estrin D.(2001), "Geographical and energy- aware routing: A recursive data dissemination protocol for wire- less sensor networks," Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech.