International Journal of Grid Distribution Computing
Vol. 8, No.6, (2015), pp.247-256
http://dx.doi.org/10.14257/ijgdc.2015.8.6.24

A Load Balancing Multi-path Secure Routing Scheme for Wireless Sensor Networks

Jianmin Zhang, Hao Li and Qingmin Cui

College of Computer, Henan Institute of Engineering, Zhengzhou 451191, China
zjm1996@163.com, lhl_103@163.com, qmcui@163.com

Abstract

Lifetime optimization and security are two important design issues for WSNs with non-replenishable energy resources. Routing protocols in wireless sensor networks (WSNs) are susceptible to a number of attacks depending on the nature of the protocol, its application, and the environment in which the protocol is intended to be used. Routing protocols that do not take the malicious attacks into account can not be easily temper proofed. The longevity of WSNs is a crucial concern that significantly influences their applicability in a specific context. In this paper, we present a Load Balancing Multi-path Secure Routing (LBMSR) protocol to address these two issues concurrently through balanced energy consumption and one-way hash key chain and symmetric key cryptography. LBMSR is designed with two configurable parameters, load balance control and security level. Load balance is used to avoid the problem of energy consuming imbalance and the formation of energy holes. Security level is designed to determine the probabilistic distribution of the random walking that provides routing security. Simulation results and security analyses show that the proposed algorithm can provide excellent balance between routing efficiency and energy consumption while preventing routing attacks.

Keywords: *wireless sensor networks; routing; security; load balancing*

1. Introduction

Wireless sensor networks (WSNs) are composed of many communication nodes with limited sensing, processing and computational capabilities and one or more data sinks located either at the center or out of the sensing field[1]. Routing is at the center of sensor networks and in recent years, many algorithms have been proposed for the routing issue in wireless sensor networks, such as GRAB [2], GEAR[3], Cluster-based routing schemes[4,5], multi-path routing scheme [6, 7], and so on However, most of these routing protocols only focus on the usability of sensor networks but neglect their security. In fact, wireless sensor networks are always deployed in hostile and unattended environments. Furthermore, multi-hop routing mechanism also has many vulnerable characters. Karlof and Wanger [8] have revealed that especially current routing protocol are insecure and are highly vulnerable to node capture attacks. Lack of security in these protocols make them vulnerable to host or routing attacks, such as spoofing, selecting routing, impersonation, wormhole, sinkhole and flood attacks. However, complex security measures based on cryptography are inapplicable owing to the calculation and storage capability of the nodes of WSNs. All of these problems pose a great security challenge to WSNs than tradition networks.

Secure routing protocols should be resilient in the presence of several compromised nodes that launch selective forwarding attacks (malicious nodes arbitrarily drop the relaying packets instead of forwarding them). Also, to protect

ISSN: 2005-4262 IJGDC

the network from the malicious nodes that inject forged routing information with an intention of routing inconsistencies, secure routing protocols should have a mechanism that detects and isolates these compromised nodes with a light-weighted security mechanism in consideration of limited capacity of sensor nodes.

Though some works have addressed the security problems in the routing protocol of wireless sensor networks, the privacy and security issues posed by wireless sensor network still represent a rich field of research problem. A properly designed secure routing protocol should not only ensure high message deliver ratio and guarantee low energy consumption for packet delivery, but should also balance the entire sensor network consumption, and thereby extend the sensor network lifetime. However, this requirement makes the secure routing in wireless sensor network even more complicated. Owing to the limited resources of sensor nodes, the security mechanism employed in wireless sensor network should be as light as possible. In this paper, we proposed a routing mechanism which realizes routing security by one-way hash key chain and symmetric key cryptography and balances network load through optimizing routing to extend the service life of the network.

The paper is organized as follows: Section 2 reviews related work. Section 3 describes the scheme in detail. In Section 4 evaluate the performance of the proposed routing algorithm via simulations and compare the results with MP-EA algorithms proposed in [6]. In Section 5 we analyze how the proposed algorithm defends Sinkhole, Wormhole, Sibyl and Selective Forwarding Attacks. And we present our conclusion in Section 6.

2. Related Works

Currently, some secure routing algorithms for wireless sensor networks have been given. In [9], a secure and energy-efficient multi-path routing protocol is proposed. This scheme use multi-path alternately as the path for communicating between two nodes and mitigate the load of sensor nodes by transferring routing related tasks to the base station.

In [10] Ahmed *et al*. proposed a novel secure real-time with load distribution (SRTLD) routing protocol that provides secure real-time data transfer and efficient distributed energy usage in WSN. The SRTLD routing protocol ensures high packet throughput and minimized packet overhead.

In [11] Ghica *et al*. proposed methodologies target the efficient handling of the information load from a two-fold perspective: by providing load-balancing, and by reducing the information load altogether, as two correlated dimensions of the lifetime problem: the energy balancing dimension, and the energy efficiency dimension respectively.

In [12] Li *et al*. proposed service-oriented architectures for wireless sensor networks (WSNs) to provide an integrated platform, where new applications can be rapidly developed through flexible service composition. In this paper, an evaluation metric, path vacant ratio, is proposed to evaluate and then find a set of link-disjoint paths from all available paths. A congestion control and load-balancing algorithm that can adaptively adjust the load over multi paths is proposed. A threshold sharing algorithm is applied to split the packets into multiple segments that will be delivered via multi paths to the destination depending on the path vacant ratio.

In [13] Wang *et al*. proposed load-balanced secure routing protocol (LSRP), a load-balanced secure routing protocol for wireless sensor networks. Based on structured topology of hexagonal mesh, hops at different directions are calculated on the optimal route for transmitting data packets in LSRP. Depending on characters of hops, the nodes can rapidly find a route among multiple optimal routes by the policy of the twice probability routing selection. Data breach is prevented by data

encryption, and data security is realized by one-way hash key chain and symmetric key authentication. LSRP offers preventions against usual attacks, and it also takes into account traffic load balance.

In [14] Yuvaraju [14] proposed a new multipath routing protocol called tSEL(Secure Energy Efficient Load Balancing Multipath Routing Protocol with Transmission Power Adjustment). Single path routing protocols may lead to holes in the network due to improper load distribution among the nodes. Multi path routing protocols will lead to better load balancing than single path routing protocols. tSEL protocol selects node disjoint multiple paths and shares load among the paths effectively by following a new load sharing mechanism. tSEL provides security through RSA public key algorithm and MD5 hash algorithm.

3. Preliminaries

3.1. System Models

Here we present some assumption for the network models used in the proposed algorithm followed by the energy models of the sensor nodes

3.1.1. Network Model: We assume that the wireless sensor networks are composed a large number of sensor nodes and a sink node. As the mobility is not mandatory in many applications of WSN, we assume that all nodes are static after deployment. The sensor nodes are randomly deployed throughout the sensor domain. All nodes generate packets periodically with a common constant period. The sink node, which has greater capabilities, can directly transmit data to any sensor node in the network, which are resource-constrained, sends data along the multi-hop route to the sink node. We consider that a sink node is security and is difficult to be compromised. And the sink node shares a unique secret key with every sensor node in the network, and that each pair of neighboring node has a unique key.

We assume that the initial energy of each node is equal. That is all nodes have the same amount of energy available at the beginning, thought it is the case that those nodes within one or two hops of the sink node consume more energy during Topology Constructing phase. Usually, energy consumption can be divided into three domains: sensing, communication, and data processing. In these three domains, energy consumption in data communication is the most. Thus we only take energy for communication into account and use the communication energy consumption model in [5, 10]

3.1.2. Energy Model: The fist order radio model [15] has been widely used for measuring the energy consumption in wireless communication. In this model, the transmitted and received energy const for transmission of a *k*-bit data packet between two *d* meter distance sensor nodes are given by the two following equations respectively.

$$E_{tx} = k \times E_{elect} + k \times E_{amp} \times d^{\alpha} \quad (1)$$

$$E_{rx} = k \times E_{elect} \quad (2)$$

Where E_{elect} denotes the energy spent by transmitter electronics, E_{amp} is the transmitting amplifier and $\alpha(\alpha \geq 2)$ is the propagation loss exponent. α is about 2 for free space and will increase due to the presence of obstacles.

3.2. Definitions

1. *living node* : a node not only has enough energy to transmit data but also it has a next hop node to transmit data;
2. *dead node* : a node doesn't have enough energy to transmit data or it doesn't have a next hop to transit data;
3. *stale node*: a node has enough energy to transmit, but it can only transmit data generated by itself or by its son nodes and can't retransmit data generate by its sibling node.
4. *parent node*: a neighbor node which is one hop from the sink node less than the given node.
5. *sibling node*: a neighbor node which has the equal hop count from the sink node with given node.
6. *son node:* a neighbor node which is one hop from the sink node than the given node.
7. *leaf node:* a node that doesn't have any son nodes.

3.3. Notations

We use the following notation to describe our protocol throughout the paper:

L_u: the ideal load of sensor u

FS_u: the set of the parent nodes of node u .

BS_u : the set of the sibling nodes of node u

SS_u : the set of the son nodes of node u

P_{uv}: the proportion of load in node u assign to its father node v

S_{uv}: the load of node u assign to its father node v

$M_1||M_2$: concatenation of message M_1 and M_2

K_{uv}: the pairwise between the node u and v

K_u: the pairwise between the node u and the sink node

3. The Proposed Algorithm

In this present we scheme in detail. The proposed algorithm consists five phases: Initialization, Topology Constructing, Load Balancing, Data Forwarding, and Routing Maintenance.

3.1. Initialization Phase

Before the sensor nodes deployed, the sink node generates a random key and applies a hash function to generate a hash chain. Suppose the random key is R_0, the hash function is H, then the key chain is R_0, R_1, … R_n , here $R_{i+1} = H^i(R_i)$ and n the maximum hop count between the sink node and sensor node. The sink node will store the hash function and the last key R_n of the key chain into all sensor nodes as the authentication key. In this phase, the sink node will generate pairwise keys with each node and stores the pair key to the node. Of course, the sink node will store all pairwise keys. And each node will be loaded with pairwise keys with its neighboring nodes by using key predistribution schemes[16,17].

Let variable h be the hop counts to the sink maintained by the node. The sink set its h=0 and the every other node sets its h=n, here n is a number that is surely greater than the maximum of hop count in WSN

3.2. Topology Constructing Phase

The routing scheme organizes the sensor nodes in different levels according to the minimum hops away from the sink node. After this process, each node is aware of its minimum hop count to sink node, and knows its parent nodes, sibling nodes and son nodes. The realization procession of topology is shown in Algorithm 1.

Algorithm 1: *WSN* Topology Constructing

1: Each unknown sensor constructs three empty lists *FL*, *BL* and *SL*

2: Sink node broadcast ID , h_0 R_0 to its neighbor nodes

/* *ID* is the identity of the sink node, *R* is the authentication key in sink node

3: **for** each node *j* in WSN after received the message broadcasted from it neighbor node *i*

4: node *j* extracts the hop count value h_i from the received message

5: **if** h_i<h_j.

6: node *j* computes $H^{h_j-h_i-1}(H(R_i))$

7: **if** $H^{h_j-h_i-1}(H(R_i)) = R_j$

8: node *j* adds node *i* to its father *FL*

9: node *j* sets R_j=H(R_i)

10: **if** h_j!=h_i+1

11: node *j* set h_j=h_i+1

12: node *j* broadcasts ID_j , h_j, R_j to its neighbor

13: **end if**

14: **end if**

15: i**f** h_i>h_j.

16: node *j* computes $H^{h_i-h_j}(H(R_j))$

17: **if** $H^{h_i-h_j}(H(R_j)) = R_i$

18: node *j* adds node *i* to its son list *SL*.

19: **else**

20: the node *j* may be compromised. node *j* reports this to the sink node.

21: **end if**

22: **end if**

23: **if** h_i=h_j.

24: node *j* computes $H^{h_i-h_j}(H(R_j))$

25: **if** $H^{h_i-h_j}(H(R_j)) = R_i$ in the received packets.

26: node *j* adds sensor node *i* to its sibling list SL

27: **else**

28: node *j* may be compromised. node *j* reports this to the sink node.

29: **end if**

30: **end if**

3.3. Load Balancing Phase

This phase aims to compute the fair load of each sensor node. The main idea of the algorithm is that each sensor node sent its load to the sink node and the sink node computes the average load of each layer. Then the sink node broadcasts the average of each layer to the sensor nodes and each sensor node adjusts its load according the average load and its load. Initially, we set the L_u sensor node u to L. P_{ui} is the reciprocal of the number of father nodes of sensor node u. The algorithm is executed as follows.

Suppose node u is a leaf node. Then node u sent its parent node v a packet containing:

$$D_u||PL_{uv}||MAC(K_{uv}, Id_u||\mathrm{L_u}||PL_{vu})$$

where, $D_u = Id_u \parallel L_u \parallel \mathrm{MAC}\ (K_u, Id_u)$

$$\mathrm{PL}_{uv} = L_u \times \frac{P_{uv}}{\sum_{i \in FS_i} P_{ui}} \tag{1}$$

When node v receives the packet from its son node u, first it verifies the receiving packet. If the packet is authentic, it add S_{uv} to its load L_v . After received the packets from all of its son nodes, it sends its parent node w a packet containing:

$$Id_v||D_v||PL_{vw}||MAC(K_{vw}, Id_v||D_v||PL_{vw})$$

where, $D_v = Id_v \parallel D_u \parallel MAC\ (K_v, Id_v)$

$$PL_{vw} = (L_v + S_{uv}) \times \frac{P_{vw}}{\sum_{i \in FS_i} P_{vi}} \tag{2}$$

After sink node receives packets from all its son nodes, it verifies the receiving packet and D_u in the receiving packets by using the pairwise keys with node. If they are all authentic, it computes the average load AL of a layer as the ideal load of this layer, and then broadcasts the ideal load AL of each layer to all nodes.

When node u receives the ideal load AL of its layer, it sends the value V needed change to its son nodes. The

$$V = (L_i - AL) \times \frac{S_{ij}}{\sum_{k \in SS} L_{ik}} \text{ ,if } L_i > AL \tag{3}$$

$$V = (L_i - AL) \times \frac{1/L_{ij}}{\sum_{k \in SS} 1/L_{ik}} \text{ , if } L_i < AL \tag{4}$$

When the node v receives the requiring changed value V from its father node u, then node v changes the P_{uv} to $P_{uv} - \frac{V}{L_i}$

After this phase, the sink node knows the load of the whole network and each node knows the F_{uv} to all its parent nodes.

3.4. Data Forwarding Phase

The sensor networks start executing its task in this phase. If a node sends a message to sink node, it chooses its next hop node according the following method. There are three case needed to be considered:

case 1: Some of its father nodes are alive. In this case, the node chooses its next hop node according to the probability of fair load. Probability of each father node being chosen is addressed by the following formulation:

$$p_{ij} = \frac{P_{ij}}{\sum_{k \in FS} P_{ik}} \tag{5}$$

Here, FS is the set of the living father nodes

case 2: None of its father node is alive, but some of its sibling nodes are alive. In this case, if the packet transmitting is generated by itself or received from its son node, the node randomly chooses one of its sibling nodes as next hop node. If the packet transmitting is received from its sibling node, this node cannot retransmit this packet and this node needs to inform its sibling nodes that it is a stale node.

case 3:. None of its father nodes and sibling nodes is alive. In this case, this node can't transmit data to other node. This node needs to inform its sibling nodes and son nodes that it has become a dead node.

3.5. Routing Maintenance Phase

After some time, the residual energy of sensor node may become unequal. To minimize the disparity in the residual energy of every node, when the energy of a node decreases a given value this node will tell its residual energy E_r to all of its son nodes. When a son node receives the residual energy of its parent nodes, the P_{ij} of the parent node is changed to $P_{ij}*E_r/E$, here E is the original energy of the node.

4. Simulation Study and Performance Analysis

In this section, we use simulations to evaluate the performance of the proposed multi-path load-balanced energy routing scheme and compare it with MP-EA algorithms proposed in [6].

4.1. Performance Metric

To evaluate the performance of the proposed algorithm, we use two performance metrics describe as follows.

1. *Power imbalance factor:* We define this metric to evaluate the energy balance characteristics of the proposed algorithm. This is expressed as the standard deviation of energy consumption of the sensor nodes and given by $S = \frac{1}{N}\sqrt{\sum_{i=1}^{n}(E_r(i) - E_{avg})^2}$ where, N is the number of sensor nodes in WSNs, $E_r(i)$ denotes the residual energy of sensor node i, E_{avg} denotes the average residual energy of all senor nodes. This metric indicates how well the traffic load/energy consumption is distributed among nodes. The smaller the value is, the better the capability the routing protocol has in balancing the energy consumption.
2. *Portion of living sensor nodes:* We define this metric to evaluate the network lifetime of WSN. This is expressed as the as the living sensor nodes to the all sensor nodes in the WSN and given by

$P = \frac{Number\ \ of\ \ living\ \ sensor\ \ nodes}{Number\ \ of\ \ all\ \ sensor\ \ nodes}$. It is measured as the living sensor nodes to all sensor networks. This metric indicates the percentage of sensor nodes that can work. It gives an indicator of sensor network lifetime.

4.2. Simulation Parameter

The key simulation parameters are summarized in Table 1.

Table 1. Simulation Parameters

Parameter	Value
Area size	$100m \times 100m$
Node numbers	200
Node placement	Uniform
Transmission range	$15m$
Location of sink	(0, 0)
Initial energy	0.5J
E_{elec}	50nJ/bit
E_{amp}	100pJ/bit/m^2
α	2
Packet length	1Kbit

4.3. Simulation Results and Discussions

Figure 1 presents standard deviation of residual energy in all living nodes between MP-EA algorithm and the proposed algorithm, the energy fairness in proposed scheme is better than that in the MP-EA algorithm. Although the energy fairness in MP-EA scheme is better than that in the proposed scheme at later time, from Figure 2 we can see that at this time there are only 74 percent of living sensor.

Figure 2 gives percent of living sensor nodes at a time. It is clear that the percent of living sensor nodes in the proposed algorithm is larger than that of in MP-EA algorithm scheme at a time. For example, after the simulation lasts 50 second, there are 94 percent of sensor nodes are alive in the proposed algorithm, while in MP-EA algorithm scheme there are only 74 percent nodes are alive. The graph also shows that the time of first dead node appearing in MP-EA algorithm scheme is earlier than that in proposed scheme. From this figure, we can get that the network lifetime of proposed algorithm is longer than of MP-EA algorithm scheme.

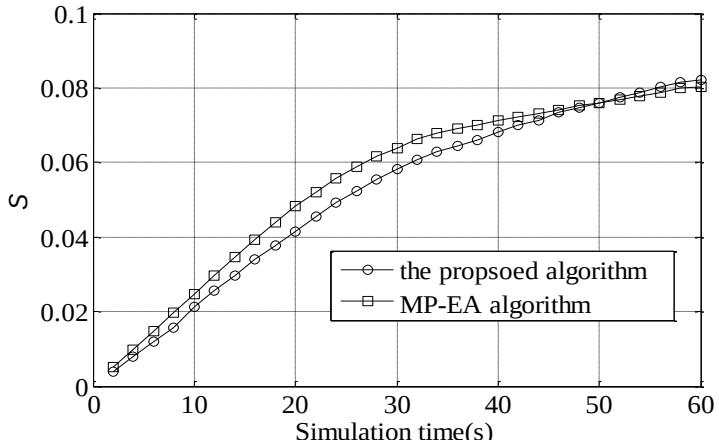

Figure 1. Standard Deviation of Residual Energy in Sensor nodes

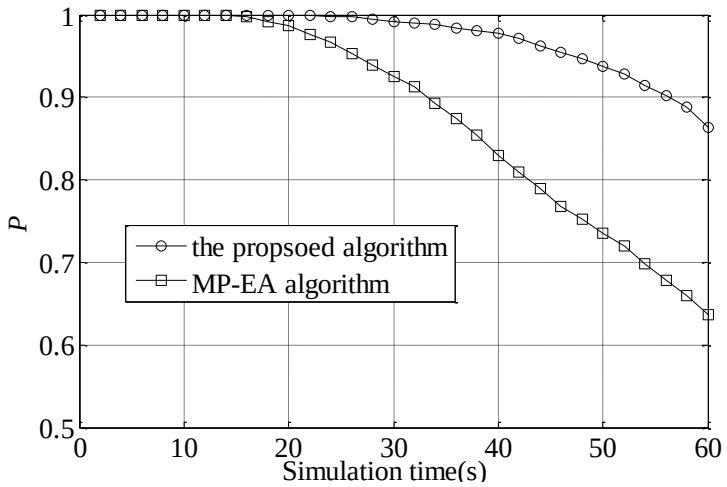

Figure 2. Portion of Living Sensor Nodes

5. Security Analyses

In this section, we describe how the proposed algorithm defends Sinkhole, Wormhole, Sibyl and Selective Forwarding Attacks.

Defending Sinkhole Attacks: In the sink hole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. In the topology constructing phase of the proposed algorithm, all sensor nodes in the network will verify the authentication of receiving packet by using the hash chain. These can prevent malicious fake the number of hop be less than the actual number. The malicious nodes can only reply or fake the hop count greater than the actual number of hops and can not do sinkhole attacks. If malicious node fake hop count greater than the actual number, it will only make it less neighbor nodes send data to it. If malicious node replies the packet replay, it will be discovered by its neighbors and being reported to the sink node.

Defending Wormhole Attacks: In the wormhole attack, ad adversary tunnels packets received in one part of the network over a low-latency link and replays them in a different part. In the proposed algorithm, all packets will be authentic by the pairwise between neighbor nodes.

Defending Sibyl Attacks: In the sibyl attack, a single node presents multiple identities to other node in the network. The sibyl attack can significantly reduce the effectiveness of fault-tolerant schemes. In the proposed algorithm, the sink will verify the packets by using the sensor *ID* and the keys between the sensor nodes and the sensor nodes. If the identify in the receiving packet are not consistent with the key stored the sink node, the receiving packet will not pass the verification

Defending Selective Forwarding Attacks: In selective forwarding attacks, malicious node refuse to forward all or part of the packets and simply drop them so that are not sent any further. In the proposed algorithm, the next node is selected based on certain probability, so the malicious nodes may be not the routing path. When the malicious nodes are not in the routing path, they cannot do selective forwarding attacks.

6. Conclusions

This paper proposed a load balancing multi-path secure routing algorithm. In this paper, we have introduced the mechanism of load balancing to balance the energy of the sensor nodes in the WSN and improve the performance in terms of network lifetime. The security is achieved via symmetric key technology, one-way hash chain. The simulation results obviously indicated that much better traffic balance effect and maximum network lifetime could be achieved with the proposed scheme and the security analyses show that the proposed routing algorithm can defend sinkhole, wormhole, sibyl and selective forwarding attacks.

References

[1] L. F. Akyidiz, W. L. Su, Y.Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communication Magazine, vol.40, no.8, **(2002)** , pp.102-114.
[2] R. C. Shah, J. M. Rabaey J M., "Energy aware routing for low energy ad hoc sensor networks", Proceeding of Wireless Communications and Networking Conference, IEEE, **(2002)** September 23-28; Chicago, IL, USA.
[3] C. Intanagonwiwat, R. Govindan, D. Estrin D, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, **(2000)** August 6-11; Boston, MA, USA.
[4] Y. Yu, R. Govindan, D. Estrin D, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department, **(2001)**.
[5] K. Du K, J.Wu J, D. Zhou, "Chain-based protocols for data broadcasting and gathering in the sensor networks", Proceeding of IEEE Parallel and Distributed Processing Symposium, 2003, **(2003)** April 22-26; Nice, France.
[6] X.Hong, M. Gerla, R. Bagrodia, T. Kwon, "The Mars sensor network: efficient, energy aware communications", Proceeding of Military Communications Conference, 2001, **(2001)** October 28-31; McLean,Virginia USA.
[7] X. Hong X, M. Gerla, H.Wang, T.Clare, "Load balanced, energy-aware communications for Mars sensor networks", Proceeding of Aerospace Conference Proceedings, 2002, **(2002)** March 9-16; Big Sky, Montana, USA.
[8] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Ad hoc networks, vol.1, no. 2, **(2003)**, pp.293-315.
[9] N. Nasser N, Y. Chen Y, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications, vo. 30, no.11, **(2007)**, pp.2401-2412.
[10] A. Ahmed, N. F.Fisal, "Secure real-time routing protocol with load distribution in wireless sensor networks", Security and Communication Networks, vol. 4, no.8, **(2011)**, pp. 839-869.
[11] G.Adviser-Trajcevski. "Extending lifetime in large scale wireless sensor networks: Secure multipath routing and load-aware tracking", Doctoral Dissertation, **(2011)**.
[12] S.Li, S.Zhao, W. Wang X, *et al*, "Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks", IEEE Systems Journal, vol.8. no.3, **(2013)**, pp. 858 – 867.
[13] X.S. Wang, Y.Z. Zhan, L.M. Wang, "Load-Balanced Secure Routing Protocol for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, vol.2013, **(2013)**, pp.1-13.
[14] M. Yuvaraju, K. Rani, "Secure energy efficient load balancing multipath routing protocol with power management for wireless sensor networks", Proceeding of 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), IEEE, pp.331-335, **(2014)**July 11-14; Kanyakumari District, India, USA.
[15] W.Heinelman , A. Chandrakasan A, H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Network", Proceeding of the Hawaii International Conference on System Sciences, **(2000)** January 4-7; Island of Maui, USA.
[16] L. Eschenauer, V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks", Proceedings of ACM Conference Computer Communication Security(CCS'02), **(2002)** November 18-22; Washington, DC, USA .
[17] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", Processing of 2003 IEEE Symposium on Security and Privacy, **(2003)** May11-14; Oakland, California, USA.

