International Journal of Engineering Researches and Management Studies

A NEW ENHANCED ENERGY EFFICIENT MULTIPATH ROUTING APPROACH FOR WIRELESS SENSOR NETWORKS

Dr. S. Saira Banu[*1] & J. Shafiq Mansoor[2]
[*1&2]Associate Professor, Department of ECS, Karpagam University, Karpagam Academy of Higher Education, Coimbatore

ABSTRACT
Wireless Sensor Network (WSN) is a group of Sensor Nodes (SNs) that work in the uncontrolled areas, organized into a cooperative network. Wireless Sensor Networks are generally composed of a large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Some of the major issues in wireless sensor networks are energy consumption, lack of authentication data integrity and instability of path link between sensor nodes which reduces the popularity of the sensor network. In recent years, the existing methods have focused on attaining either energy consumption or security. The research work consists of optimized multipath routing, residual energy based routing approach to make the wireless sensor networks more secure with minimum energy consumption. The multipath routing is constructed to achieve high throughput and load balancing. The optimal energy path is established to maintain the data packet flow in the wireless sensor network unobstructed and the energy consumption model is developed to produce the minimum energy consumption.. Residual Energy based Multipath Routing Approach is proposed which attains the integrity and minimum residual energy. It uses load balancing to prevent congestion problems in the network and the path stability is established based on link cost, link quality and bandwidth of the link.

Keywords: Wireless Sensor Networks, Multipath Routing, Energy Consumption, Data delivery ratio, Load Balancing, throughput and link quality.

1. INTRODUCTION

A. Wireless Sensor Networks (WSNs)
A sensor network consists of a large number of densely deployed sensor nodes. Wireless Sensor Networks have attracted lots of attention in recent years due to their wide applications such as battlefield surveillance, smart home, healthcare, inventory, wildlife monitoring, etc. Each node has processing capability with a radio, sensors, memory and a battery. Since the sensor nodes are usually operated by limited battery power which may not be replaced once deployed, it is therefore vital that the sensor network is energy balanced in order to ensure an extended network lifetime and efficient data gathering. Due to the severe energy constraints of large number of densely deployed sensor nodes, it requires a suite of network protocols to implement various network control and management functions such as synchronization, node localization and network security.

B. Routing in Wireless Sensor Networks
Based on the application, different architecture, goals and constraints have been considered for WSNs. Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like Mobile Ad hoc Networks or Cellular Networks. Due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high. The traditional IP-based protocols may not be applied to WSNs. Furthermore, the Sensor Nodes that are deployed in an ad hoc manner needs to be self-organized. The Ad-hoc deployment of these nodes requires the system to form connections and cope with the resultant nodal distribution. Second, in contrast to typical communication networks, almost all the applications of sensor networks require the flow of sensed data from multiple sources to a particular Base Station (BS). This, however, does not prevent the flow of data which are in other forms (e.g., multicast or peer to peer). the sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Thus, they require careful resource management.In the multipath routing, a packet traverses from a source node to a target node via several paths

International Journal of Engineering Researches and Management Studies

Problem Statement

Wireless Sensor Networks has gained world-wide attention in recent years due to the advancements in wireless communication, information technologies and in the field of electronics. The routing in the wireless sensor networks is a demanding assignment. This assignment may lead to a number of routing protocols which effectively use the limited resources available at the sensor nodes. So, all the routing protocols will attempt to find the optimal energy path. In Wireless Sensor Networks, when the Source Node sends a packet to the destination node, the intruder may eavesdrop the message that is carried by the packet. Some intruders may cause misrouting, false packet injection and the packet loss. So retransmissions will occur unnecessarily. Thus the node consumes more energy after the packet sending and receiving period. The sensor nodes are attacked by several attacks like data tampering, cipher text attack and denial of service attack. The sensor nodes are totally distributed in a random manner. The control may be issued by base station or without any base station.

The sensor nodes have limited battery life. The node has to sustain itself on its battery's limited energy resources and without power management it can last only for a short period of time. To minimize the energy consumption, there is a need of scheduling in sensor networks. Due to the mobility of nodes, packets are dropped and the performance of the networks is totally degraded.

2. RELATED WORK

Senthil kumar et.al [1] analyzed the base station which is used to provide individual base station attacks or sensor node compromises problem to design a sensor network routing protocol that satisfies the proposed security goals. One aspects of sensor networks organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes.

Sabarinathan et.al [2] proposed approach mechanisms that generate randomized multi-path routes, even if the routing algorithm becomes known to the adversary, the adversary cannot pinpoint the routes traversed by each packet. Instead of splitting message into shares, here splitting message into packets and applying MD5 algorithm to provide additional security. The proposed approach provides confidentiality, minimize packet interception probability and end-end energy consumption, the additional features provide solutions to cut-around sink attack.

Shuang Li et.al [3] proposed a multipath based on directed diffusion that reinforces multiple routes with high link quality and low latency. This algorithm retains the merits of the original directed diffusion algorithms, including its energy efficiency and scalability. They used the NS-2 simulation tool with video trace generated by Multiple Description Coding (MDC) to evaluate the performance. The results show that our algorithm gives better throughput and delay performance.

Hamid reza Hassaniasl et.al [4] proposed Score-Aware Routing Algorithm (SARA) is used to enhance routing quality. For that, they have analyzed the five factors like distance between each node and sink, number of observed sources by each node, remaining energy in each node and reliability of communication link and value of traffic in each node. It was more efficient in terms of decreasing delay, decreasing the number of lost packets, improving the load distribution and purposeful network lifetime.

Yuxin Mao and Guiyi Wei [5] proposed a novel approach of secure data collection for wireless sensor networks. They presented a novel tracing-feedback mechanism, which makes full use of the routing functionality of wireless sensor networks, to improve the quality of data collection. The major advantage of the approach is that the secure paths are constructed as a by-product of data collection. The process of secure routing causes little overhead to the sensor nodes in the network.

S. Saqaeeyan and M. Roshanzadeh [6] proposed optimum routing protocol, in some of Quality of Service achieved improvements in the field of reliability in data sending to destination and load balancing in wireless sensor network. In the proposed protocol, to ensure that a data packet correctly send to the destination, it used of an improved hybrid method based on multipath data sending. The routing decisions in this method are by considering the remaining energy of nodes that are in neighbors of sender nodes.

IJERMS
International Journal of Engineering Researches and Management Studies

Riyaz Pasha et.al [7] presented model of self-optimized multipath routing algorithm for WSN and its results. mechanism is based on delay, energy and velocity. The adopted factors and reinforcement learning (RL) feature help WSN in improving the overall data throughput; especially in case of real time traffic. The algorithm is also capable to avoid permanent loops which promotes dead lock problem in the running networks.

S. Ganesh and R. Amutha [8] developed a comprehensive approach to understand the fundamental performance of information routing in energy-limited wireless sensor networks through optimal Signal to Noise Ratio (SNR) based power control mechanism and optimal handoff-based self-recovery features. They presented some results for a few different small-scale WSN experiments to study the solutions obtained for these problems.. Based on the simulation results, they concluded that efficient and secure routing protocol (ESRP) with optimal power control mechanism and handoff-based self-recovery can significantly reduce the power usage.

Reza Azarderskhsh and Arash Reyhani-Masoleh [9] proposed a new secure clustering scheme for clustered WSNs incorporating public key cryptography. They take an advantage of gateway nodes which are powerful and tamper proof to establish/revocate the symmetric keys in each cluster. This key establishment is completed during the bootstrapping and clustering phase assuming that the adversary is present in the field. It was presented an approximation to determine the number of neighbor nodes for each sensor node obtained from the average number of neighbor nodes involved in the routing algorithm toward the gateway

Saira Banu, and R.Dhanasekaran [10] proposed a New Multipath Routing Approach (NMRA) for increasing the energy efficiency in WSNs. In WSNs, the best route is being determined by choosing efficient strategy to forward the data to the base station. Due to that, the node consumes more energy unnecessarily. In this method a New Multipath Routing Approach was developed which attains energy model, maintenance of optimal energy path, multipath construction phase to make a correct balance between network life time, energy consumption and throughput to the sensor nodes.

3. IMPLEMENTATION OF PROPOSED ALGORITHM

The proposed Multipath routing scheme consists of three steps like multipath construction phase, maintenance of optimal energy path and the energy consumption model to improve the energy efficiency in the sensor networks.

A. Multipath Routing

In the multipath routing, a packet traverses from a source node to a target node via several paths. The main goal is to increase reliability, as a packet can be received via an alternative path even if the routing in some path fails. However, the multipath routing has a trade-off between the reliability and energy, as it increases network load and energy usage due to the extra transmissions Each packet is assigned with a budget that is initialized by the source node.

The budget consists of the minimum cost to send a packet to the sink and an additional credit. When a node receives the packet, it compares remaining budget against the cost required to forward the packet to the sink. If the cost is smaller or equal to the budget, the node forwards the packet. As the credit increases the budget, it allows forwarding the packet along the other minimum cost paths. Thus, the credit determines the amount of redundancy for the packet and has a trade-off between used energy and reliability. If the credit is zero, the packet must be forwarded along the minimum cost path

Multipath routing in conjunction with hop-to-hop authentication results in multipath authentication. A message is sent over multiple, strictly disjoint, paths. If different versions of a message are received, the recipient chooses the majority version. All other paths can be markes as untrustworthy, since they delivered a presumably incorrect message.. Some nodes may be only loosely connected to the network and cannot profit from multipath routing. It is more demanding to find and maintain sets of disjoint paths between two communication endpoints, compared to a single path.

The proposed multipath system in figure1 uses multi-path routing in order to select the route with the best maximum data throughput rate.

IJERMS
International Journal of Engineering Researches and Management Studies

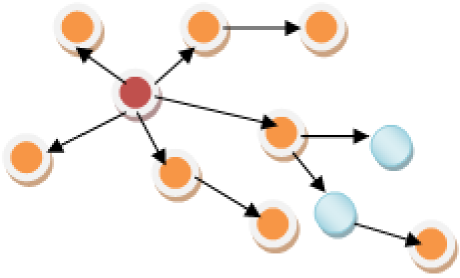

Fig.1. Mulitpath Routing Approach

B. Maintenance of optimal multipath

The concept of optimal energy path is used to appraise the minimum energy consumption. The main aim is to maintain the data packet flow in the wireless sensor network unobstructed. The definition of the sensor network model is given as follows.

Let us assume a given network $N(\Psi,\Theta)$ is composed of Ψ and Θ, where Ψ is the set of nodes and Θ is the set of links. Due to the feature of multi-hop transmission, sensor network could have many paths from source node *s* to destination node *d*. Therefore, Let Π (*s*,*d*) denote the set of all possible paths starting from *s* to *d*. According to these definitions, it is known that Π (*s*,*d*) is the subset of Λ.

Let $\boldsymbol{\pi}$ represents a generic path, and $\boldsymbol{\pi}i(s, d)$ represents the *i*-th path in a journey from source node *s* to destination node *d*. Also,

Let $\Phi(\boldsymbol{\pi})$ be a generic cost function associated to a designated path $\boldsymbol{\pi}$. $\Phi(\boldsymbol{\pi})$ can be the delay time $\theta(\boldsymbol{\pi})$ for a packet which transfers through a path $\boldsymbol{\pi}$, or the number of hops $\varepsilon(\boldsymbol{\pi})$, even a hybrid function combined both of them. If it possesses the same cost for two or more paths, consider them as Φ-equivalent. Since each node in the WSN functions as a router that works independently, several connection matrices are defined and stored in each node to help performing the energy efficient routing function.

If the Connection matrix is denoted as *Ts* = (*ts,d*) where *Ts* is an array that registers all outgoing links of node *s*, and *ts,d* determines whether node *s* has an outgoing link connected to node *d* or not, 1 represents connected, 0 represents disconnected.

Let *Bs,d* denotes the bandwidth utility ratio of link from node *s* to node *d*. *ps,df* determines the probability table for deciding the next node of a packet transferring from node *s* to its final destination node *df*. *ps,df,j* corresponds to the probability for the packet transferred to node *j*. Note that $\Sigma j(ps,df,j) = 1$. Also, suppose *E*full is the initial energy on each node and *Ej* is the remaining energy on node *j*. The weight of choosing node *j* as the next node for transferring the packet while the packet is queued at node *s* is,

$$W(s,j,df)=t_s,j(ps,df,j)^{C1}(1-B_s,j)^{C2}(E_j/E_{full})^{C3} \qquad (1)$$

where *C1, C2 and C3* are weighting factors that regulate the importance of probability matrix (*ps,df*), bandwidth utility ratio (*Bs,j*), and remaining energy ratio (E_j/E_{full}) during routing process, respectively.

The values of *C1, C2 and C3* are set as 1 in most cases. Supervisors can obtain desired performance by adjusting these parameters. There is no systematic approach to obtain the optimal values of these parameters since it involves too many human factors. Hence, generally, we set the values of C_1, C_2, and C_3 to 1. The probability of choosing node j as next node of the packet can be defined as follows

$$\sigma_{s,j} = \frac{w(s,j,df)}{\sum_{\forall h} w(s,h,df)} \qquad (2)$$

IJERMS
International Journal of Engineering Researches and Management Studies

The load-balance feature of the proposed scheme can be exploited using Equation (3.2) and is a normalized firing strength to send a packet from a node *s* to node *j*. This equation contains the terms of bandwidth utility ratio *(Bs,j)* and remaining energy ratio (*Ej/Efull*). In the investigation, once the packets reaches to its final destination node through the path $\pi i(s,d)$, the cost function of the path can be defined as follows

$$\phi(\pi i(s,d)) = \theta(\pi i(s,d)) \tag{3}$$

The possibility of selecting a path $\pi i(s, d)$ to transfer a packet from node *s* to node *j* is updated by the following equation,

$$\Delta p_s, d_f, j = \begin{cases} (\frac{Q}{\Phi(\pi i(s,j))})^{[if\,(s,j)\subset \pi i(s,d)]} \end{cases} \tag{4}$$

Where Q, an awarding amount, is constant and can be any value. Therefore, we can update the probability matrix *ps,df* according to the following equation

The normalization can be performed on p_s, d_f using,

$$p_s, d_f, j = \frac{p_s, d_f, j}{\sum_{\forall h} p_s, d_f, h} \tag{5}$$

These parameter updating procedures will be executed once a packet reaches its destination node.

C. Determination of Path Stability

Let *Nb* denote the neighbor set of node *b* and node *b* will choose the next hop by following the criterion

$$L_{ct} = \arg\min_{l \in N_b} \begin{cases} (1 - \frac{e_{j,remaining}}{e_{j,init}})^{[\delta(1 - \frac{(\Delta dh+1)}{d_{oe}})]} \end{cases} \tag{6}$$

where d_{oe} is the distance in hops between node *o* and sink e;
d_{ke} is the distance in hops between node *k* and sink e;
Δdh is the difference between d_{oe} and d_{ke}
$e_{j,init}$ is the initial energy level of node *j*
$e_{j,remaining}$ is the remaining energy level of node *j*; and
δ is the weight factor and $\delta > 1$.

Note that $(\Delta dh+1) \in \{0, 1, 2\}$ and $(1-e_{j,remaining}/e_{j,init}) \in (0, 1)$. The link cost function takes both the node energy level and hop distance into account.

Suppose $e_{j,remaining}$ remains constant. In this case, the link cost increases when $(\Delta dh+1)$ increases. On the other hand, suppose $(\Delta dh+1)$ remains constant. In this case, the link cost increases as $e_{j,remaining}$ decreases.

The weight factor δ adjusts the priority. A large δ gives more weight to the node energy than to the hop distance

D. Energy Consumption Model

The energy consumption of idling is always spent by the nodes to avoid collisions, which is the function of MAC layer. layer. The total energy consumption can be considered as the energy consumption of sending and receiving a packet multiplied by the total transmission times. The sending energy ETX (k, d) and the receiving energy ERX (k) become the focus. In wireless networks, as long as the nodes are deployed in the transmission

IJERMS
International Journal of Engineering Researches and Management Studies

range of the transmitting nodes, they receive these packets for free even if these packets do not belong to their duties. This phenomenon is considered as the broadcasting characteristic of wireless networks. So, the total energy consumption is

$$E_{MULT} = (E_{TX}(k, d)) + N \times (E_{RX}(k)) \times NR \qquad (7)$$

Where N is the number of nodes in a cluster, NR is the transmission times in the network, k is the packet size, and d is the transmission radius.

To simplify the discussion, it is assumed that all the sensor nodes have the same transmission radius. The relationship among energy consumption, packet size k, and transmission radius d for one node is

$$E_{TX}(k, d) = k \times E_{txElec} + k \times \delta\, amp \times d\gamma + E_{start} \qquad (8)$$

Where E_{txElec} is the energy of sending one bit data. It is the path loss factor whose value is constant in a typical condition. δ amp is the value of signal amplifier, and E_{start} is the energy consumption of starting transmission. On the other hand, the energy consumption of receiving is

$$E_{RX}(k) = k \times E_{rxElec} + E_{star} \qquad (9)$$

E_{rxElec} is the energy consumption of receiving one bit data.

$$E_{rxElec} = E_{txElec} = E_{elec} \qquad (10)$$

Table 1. Simulation Settings and Parameters of Proposed NMRA Scheme

No. of Nodes	200
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	5 pkt/s
Protocol	DSR

Table 2 Comparison Results of Proposed NMRA Scheme and Existing Scheme

Performance Metrics	NMRA	SBYaoGG
Energy Consumption (Joules)	700-580	1300-800
Network Lifetime (Secs)	223.56-440.33	100.45-347.89
Overhead (pkts)	0.32-0.75	0.88-1.34
End to End delay (msec)	0.42-0.85	0.678-1.15
Data Availability (pkts)	950-4800	500-2300

International Journal of Engineering Researches and Management Studies

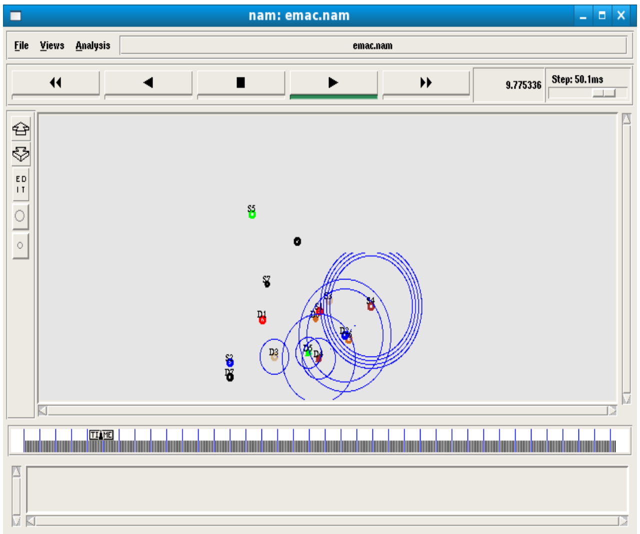

Figure 1. Topology of the proposed scheme

Figure 1 shows that the proposed scheme topology for ensuring the multipath routing. Source node sends the packet to destination node via intermediate nodes. In case if the node failure occurs, the node choose the alternative path to reach correct delivery of packets.

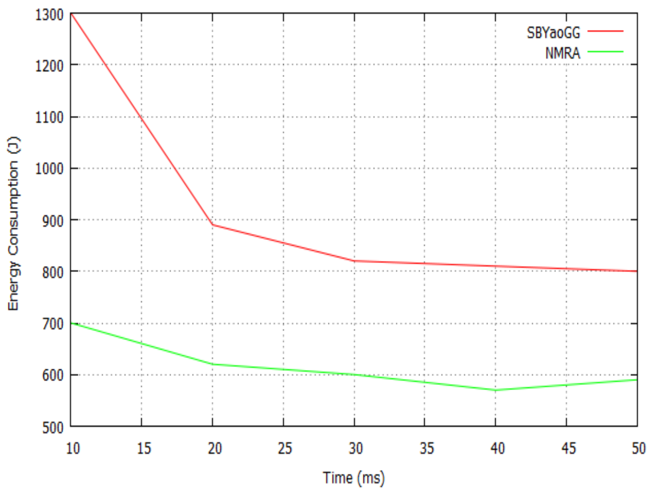

Figure 2 Time Vs Energy consumption using NMRA Scheme

Figure 2 shows the results of average residual energy by varying the time from 10 to 50ms. From the results, it shows that NMRA scheme has minimal energy consumption than the existing scheme SBYaoGG.

4. Conclusion

The proposed New Multipath Routing Approach attains energy model, maintenance of optimal energy path, multipath construction phase to make a perfect balance between network life time, energy consumption and throughput to the sensor nodes. The simulation tool is used to show the performance of proposed scheme. The proposed scheme uses the factors such as path stability, residual energy and authenticity for packet forwarding by maintaining high residual energy consumption and secure routing to each sensor node. The proposed scheme attains the integrity, minimum residual energy and achieves better performance than the existing schemes.

IJERMS
International Journal of Engineering Researches and Management Studies

REFERENCES

1. *A.Senthilkumar and Dr.C.Chandrasekar, "Secure Routing in Wireless Sensor Networks: Routing Protocols", International Journal on Computer Science and Engineering. Vol. 02, No. 04, 2010, pp.1266-1270.*
2. *Sabarinathan K and Ramesh S, "Secure Data Delivery in Wireless Sensor Network Using Collaborative Randomized Dispersive Routes", Journal of Computer Applications, 2012, Volume-5, Issue2, pp.174-178.*
3. *Shuang Li, Raghu Kisore Neelisetti, Cong Liu and Alvin Lim, "Efficient Multi-path protocol for Wireless Sensor Networks", International Journal of Wireless & Mobile Networks, Vol.2, No.1, 2010, pp.110-130.*
4. *Hamid reza Hassaniasl, Amir masoud Rahmani, Mashaallah Abbasi Dezfuli and Arash Nasiri Eghbali, "A Novel Score-Aware Routing Algorithm in Wireless Sensor Networks", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (5), pp.397 – 404.*
5. *Yuxin Mao and Guiyi Wei, "A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection", Sensors, 2010, Vol.10, pp.9529-9540*
6. *S. Saqaeeyan and M. Roshanzadeh, "Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks", International Journal of Computer Network and Information Security, 2012, Vol.2, pp.8-14.*
7. *M.Riyaz Pasha and B.V.Ramana Raju, "A Self-Optimized Multipath Routing Protocol forWireless Sensor Networks", International Journal of Advacnes in Computer Networks and its Security, pp.203-207.*
8. *S. Ganesh and R. Amutha, "Efficient and Secure Routing Protocol forWireless Sensor Networks through Optimal Power Control and Optimal Handoff-Based Recovery Mechanism", Journal of Computer Networks and Communications, Article ID 971685, pp.1-8.*
9. *Reza Azarderskhsh and Arash Reyhani-Masoleh, "Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking, Volume 2011, Article ID 893592, pp.1-8.*
10. *Saira Banu and Dr. R.Dhanasekaran, " A New Multipath Routing Approach for Energy Efficiency in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887), Volume 55, No.11, 2012, pp.24-30..*