AN ENHANCED ENERGY EFFICIENT SECURE MULTIPATH ROUTING SCHEME FOR WIRELESS SENSOR NETWORKS

[1]S.SAIRA BANU, [2]KALVIKKARASI.S, [3]ARUNA.R

[1]Associate Professor, Department of Electronics, Karpagam Academy of Higher Education, India
[2,3] Research Scholar, Department of Electronics, Karpagam Academy of Higher Education, India
E-mail: [1]sairabanu.ecs@gmail.com

Abstract: Wireless Sensor Networks are generally composed of 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. The research work consists of optimized multipath routing, residual energy based routing, authentication and scheduling based approach to make the wireless sensor networks more secure with minimum energy consumption. 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. A New Scheduling based Energy Efficient Scheme is established which attains both throughput and peak network connectivity while keeping the nodes moving in dynamic manner.

Keywords: Wireless Sensor Networks, Multipath Routing, Optimum Energy Path, Network Life time, Energy Consumption

I. INTRODUCTION

Wireless Sensor Networks(WSN) have gained world-wide attention in recent years due to the advances made in wireless communication, information technologies and electronics field. Wireless sensor network generally composed of a large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Each network is equipped with more than one sensors, processing units, controlling units, transmitting units etc. A sensor network consists of a large number of densely deployed sensor nodes. The position of the sensor nodes is not usually predetermined, as the network may be deployed in inaccessible terrains or disaster relief operations. Compared to ad hoc networks, sensor networks have some unique feature and application requirements..

Design goals of Wireless Sensor Networks WSNs)
Based on the application, different architecture, goals and constraints have been considered for WSNs.

a. Energy Considerations
During the creation of an infrastructure, the process of setting up the routes is greatly influenced by energy considerations. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Most of the time sensors are scattered randomly over an area of interest and multi-hop routing becomes unavoidable.

b. Node deployment
Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

c. Energy consumption without losing accuracy
Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

d. Quality of Service
In some applications, data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

Security goals and threats of Wireless Sensor Networks WSNs)

Based on the application, different architecture, goals and constraints have been considered for WSNs.

a. Eavesdropping
Eavesdropping occurs when an attacker compromises an aggregator node and listens to the traffic that goes

through it without altering its behavior. Since aggregator nodes process various pieces of data from several nodes in the network, it does not only leak information about a specific compromised node, but from a group of nodes.

b. Data tampering and packet injection

A compromised node may alter packets that go through it. It may also inject false messages. Since an aggregate message embeds information from several sensor nodes, it is more interesting for an attacker to tamper with such messages than simple sensor readings..

c. Ciphertext attack

It is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts.

Problem Statement

In wireless sensor networks, the sensor nodes are attacked by several attacks like eavesdropping, data tampering, false packet injection and denial of service attack. When the source node sends a packet to destination node, the intruder may eavesdrop the message that is carried by packet. Some intruders may cause the misrouting, false packet injection and packet lost. Because of the incorrect path stability, the intruders may arise and misuse the information. So the retransmission will occur unnecessarily. Thus the node consumes more energy after packet sending and receiving period. To reduce the effects of eavesdropping, data tampering, ciphertext attack, false packet injection and denial of service attack, the stability of path is undertaken here. In addition to this, we calculate the residual energy of the sensor node once the packet loss or discard or any bad packet error sent or received. This calculation determines the efficiency of our proposed scheme. To minimize the energy consumption, there is a need of scheduling in sensor networks. For that we proposed multipath routing based scheduling mechanism to make a correct balance between the network connectivity and energy efficiency.

II. 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 aspect 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. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. 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. A hybrid metric of link quality and latency is used as the criterion for path selection. In order to select disjoint paths, we propose a scheme for reinforced nodes to respond negatively to multiple reinforcement messages. 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, i.e higher video quality, than standard directed diffusion that transmits over a single path, with low overheads and energy consumption.

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 shown that with higher network density or higher number of sources and higher rate of sent data, the efficiency of the developed algorithm would increase, and such increase is due to the higher number of nodes suitable for selection for routing.

III. IMPLEMENTATION OF PROPOSED ALGORITHM

a. Concept of Proposed Multipath Routing

The New Multipath Routing Approach (NMRA) is proposed for increasing the energy efficiency in WSNs. Our proposed Multipath routing scheme consists of 3 steps like multipath construction phase, Maintenance of optimal energy path and Energy consumption model to improve the energy efficiency in Sensor networks. The concept of proposed multipath feature is towards broadcasting the traffic load among two or more routes. The proposed multipath system uses multi-path routing in order to select the route with the best maximum data throughput rate.

b. Determination of Path Stability

In order to reduce the effect of DoS attacks, Data tampering and Eavesdropping, the stability of path is undertaken here. Path stability includes the link cost, link quality and bandwidth of the link. The link cost function is used by the node to select the next hop

during the path search phase. Let N_b denote the neighbor set of node b, node b will choose the next hop by following the criterion.

$$L_{ct} = \arg\min_{l \in N_b} \left\{ (1 - \frac{e_{j,remaining}}{e_{j,init}})^{[\delta(1-\frac{(\Delta dh+1)}{d_{oe}})]} \right. \quad (1)$$

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 $\delta > 1$.

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.

Link quality is determined from received signal strength value and signal to noise ratio value. Here we include the packet dropping ratio for determining the path quality. It is defined as the number of packets dropped to the total number of packets received in the particular link. Bit Error Rate is inversely proportional to the SNR. The SNR is derived as

$$SNR = \frac{S_R}{\sum_{i \neq R} P_u + N_K} \quad (2)$$

where the vector denotes the traffic rates allocated to all available routes and f_j is the traffic flow allocated to path j.

The idle period of the wireless channel is a key parameter to determine the average bandwidth which is determined by the traffic travelling along the mobile nodes as well as their neighbor nodes. During that period the mobile nodes can successfully transmit data packets.

$$Avg_{bw} = Max_{bw} \otimes \left(\frac{Idle_t}{Initial_t} \right) \otimes L_q \quad (3)$$

Where L_q is the link quality.

The proposed Residual Energy based Multipath Routing Approach(REMRA) attains the integrity and minimum residual energy.

Determination of Remaining energy

After periodical time t, the energy consumed by the node $E_{j,\ remaining}$ is calculated as follows.

$E_j = \chi \times T_{nx} + \lambda \times R_{nx}$ (4)

Where T_{nx} = Number of data packets transmitted by the node after periodical time t. R_{nx} =Number of data packets received by the node after time t χ and λ are constants. Its value ranges between 0 and 1. If E_{INIT} is the initial energy of a node, the remaining energy $E_{remaining}$ of a node at periodical time t, can be calculated as:

$E_{j,\ remaining} = E_{j,INIT} - E_j$ (5)

c. Integrated Encryption/Decryption Scheme (IEDS)

Efficient Multipath Routing based Cryptography Scheme(EMRCS) guard against the ciphertext attacks and all known attacks. In our multipath approach we use the concept of Elliptic Curve Cryptography. In IEDS, a Diffie-Hellman shared secret is used to derive two symmetric keys k1 and k2. Key k1 is used to encrypt the plaintext using a symmetric-key cipher, while key k2 is used to authenticate the resulting ciphertext.

d. Scheduling algorithm

The proposed New Scheduling based Energy Efficient Scheme (NSEES) attains both throughput and network connectivity while keeping the nodes moving in dynamic manner. Here D_{max} is the maximum node connectivity, w is the code weight, q is the number of codewords with different weights and N is the number of mobile nodes participated in the network.

Step1 : Initially set the code weight $w = D_{max} + 1$.

Step 2: Determine the distance from source to destination node.

Step 3: Set the initial link schedule to zeros.

Step 4: Choose the highest link scheduling priority

Step 5: Compute ON (t_{ON})and OFF time (t_{OFF}).

Where t_{ON} is the maximum time for the node to sleep thoroughly before the routing establishment, also it is the minimum time to reach the destination node with the maximum speed.

$$t_{ON} = \frac{f - r}{v_{max}} \quad (6)$$

t_{OFF} is the maximum time for the node to pass by the node's transmission range, but if the node moves out of the region with a shorter time than the expected passing by time, the scheduling can be recovered, thus

$$t_{OFF} = \min \left\{ \frac{f + r}{v_{min}}, t_{exp} \right\} \quad (7)$$

t_{exp} is time expiration that node move out of the cluster.

V_{min} is the minimum speed of the node.

Step 6: Each node in CH_1 is assigned with a unique codeword in Q_1 and each node in CH_2 is assigned with a unique codeword in Q_2.

Step 7: Compute the included angle ϕ between the root node connection line and the instant velocity v.

Step 8: Compute maximum network connectivity ratio DC_{max}. DC_{max} will increase as the node's instant speed and the direction probability increase.

For the normal distribution model,

$$DC_{\max} = \frac{e.v}{\sqrt{2\pi(pv+q)}} \exp(-\frac{\theta^2}{2(pv+q)}) + k \quad (8)$$

e – energy of the node, V-vector

θ - Inclined Angle, p,q – Axes, k - Approximate value

Step 9: Each node transmits its data packets only at its assigned slots determined by its codeword.

Step 10: Once the scheduling is complete, the active links will transmit data according to the scheduling result.

e. Determination of Energy Conservation Ratio

The proposed algorithm determines the energy conservation rate based on the above three factors and also the total number of bits transmitted per energy.

$$E_{CR} = \sum(T_{mb}, T_{tv}, DS_{\min}) + \frac{\chi_{BR}}{\sum \delta_{es}(t)} \quad (9)$$

χ_{BR} - Number of bits transmitted (bits).

$\sum \delta_{es}(t)$ - Total energy consumed (Joules).

T_{mb} – Trust Mobility factor

T_{tv} – Trust threshold vector value

DS_{min} - Minimum Digital Signature

By limiting the factors like mobility, malicious activities, unauthenticated node occurrence and bits transmitted per energy, the node energy consumption can be reduced.

IV. PERFORMANCE ANALYSIS

We use Network Simulator (NS 2.34) to simulate our proposed algorithm. Network Simulator-2(NS2.34) is used in this work for simulation. Networks. In our simulation, 200 mobile nodes move in a 1200 meter x 1200 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in Table 1.

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. 1 Simulation settings and parameters of proposed algorithm.

Figure 1.1 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 Figure 1.2 shows the results of average residual energy for varying the time from 10to50ms. The REMRA scheme has minimal energy consumption than the NMRA, AFTMR[72] and SBYaoGG schemes

Figure 1.3 presents the comparison of network lifetime. The network lifetime of REMRA is higher than the NMRA, AFTMR [72] and SBYaoGG [38] Schemes.

Figure 1.4 shows the results of Time Vs End to End Delay. The EMRCS scheme has slightly lower delay than the NMRA, AFTMR and SBYaoGG schemes because of the authentication routines.

Figure 1.5 presents the comparison of network lifetime on NSEES with other existing schemes.. The network lifetime of NSEES is higher than the NMRA, AFTMR and SBYaoGG and DMP Schemes.

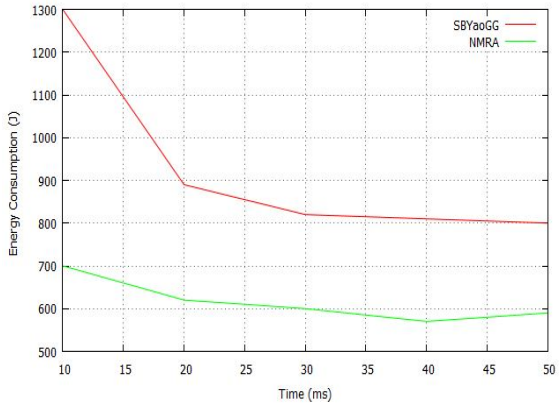

Figure 1.1 Time Vs Energy consumption using NMRA Scheme

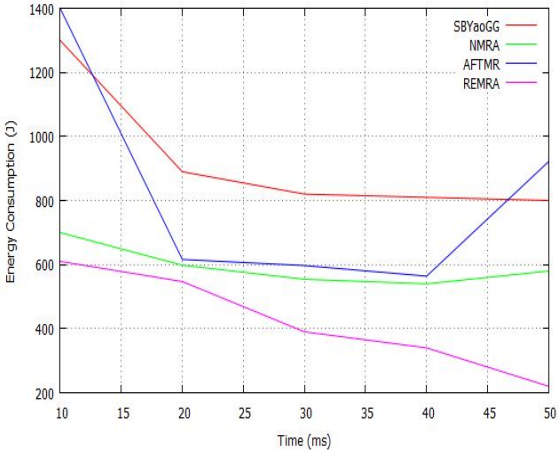

Figure 1.2 Time Vs Energy Consumption using REMRA Scheme

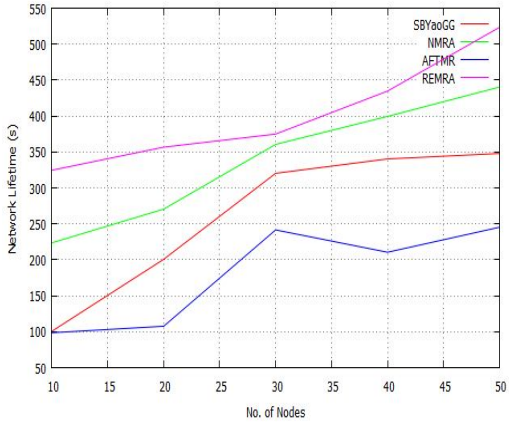

Figure 1.3 No. of Nodes Vs Network Lifetime using REMRA Scheme

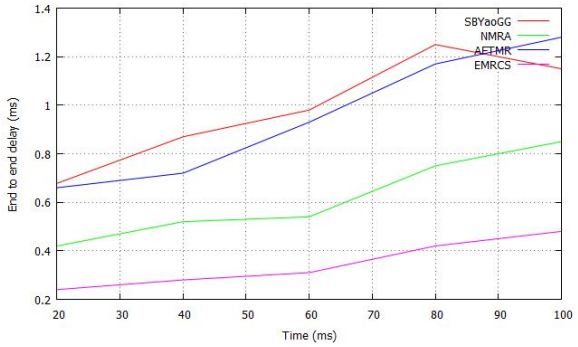

Figure 1.4 Time Vs End to End Delay using EMRCS Scheme

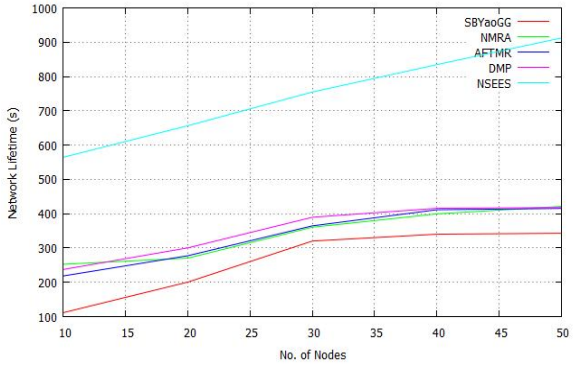

Figure 1.5 No. of Nodes Vs Network Lifetime using NSEES Scheme

CONCLUSIONS

A New Multipath Routing Approach (NMRA) is developed which attains energy model, maintenance of optimal energy path, multipath construction phase to make a correct balance between the network life time, the energy consumption and throughput to the sensor nodes. A Residual Energy based Multipath Routing Approach (REMRA) was developed which attains correct balance between the energy consumption and the authentication to the sensor nodes. In the first phase of the scheme, concept of proposed multipath routing is explained. In the second phase, the path stability is determined to ensure the network connectivity. An Efficient Multipath Routing based Cryptography Scheme (EMRCS) developed which attains the correct balance between energy consumption and authentication to the sensor nodes. The proposed NSEES scheme is to provide the multipath routing based scheduling to maximize the network connectivity ratio and throughput. By using NS 2.34, a discrete event simulator, the NMRA, REMRA, EMRCS and NSEES scheme achieves high connectivity ratio and delivery ratio, low overhead, low end to end delay and minimum energy consumption while varying the time, throughput, number of nodes and mobility than the existing schemes such as SBYaoGG, AFTMR and DMP.

REFERENCES

[1] A.Senthilkumar, Chandrasekar, "Secure Routing in Wireless Sensor Networks: Routing Protocols", International Journal on Computer Science and Engineering. Vol. 02, No., pp.1266-1270, 2010

[2] Sabarinathan K and Ramesh S, "Secure Data Delivery in Wireless Sensor Network Using Collaborative Randomized Dispersive Routes", Journal of Computer Applications, Volume-5, Issue2, pp.174-178, 2012.

[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, pp.110-130, 2010.

[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, 2010

[5] Yuxin Mao and Guiyi Wei, "A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection", Sensors, Vol.10, pp.9529-9540, 2010.

[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] Saira Banu and R.Dhanasekaran, " A New Multipath Routing Approach for Energy Efficiency in Wireless Sensor Networks", International Journal of Computer Applications, Volume 55, No.11, pp.24-30, 2012

[10] Reza Azarderskhsh and Arash Reyhani-Masoleh, "Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking, Article ID 893592, pp.1-8, 2011

[11] S.Saira Banu and R.Dhanasekran, "A New Residual Energy Based Multipath Routing Approach for Wireless Sensor Networks", European Journal of Scientific Research, Vol.95, No.2,January 2013, pp. 168 - 179.

★★★