ISSN:0975-9646

An Approach towards Improving the Lifetime and Security in Wireless Sensor Network

Mayuri P. Kawalkar[1], Dr. S.A.Ladhake[1]

[1]*Information Technology ,*[2]*Electronics & Telecommunication,*
S.G.B.A.University,
Amravati, Maharashtra ,India

***Abstract*— A Wireless Sensor Network (WSN) is a collection of wireless sensor nodes forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, due to the limited range of each node's wireless transmissions, it may be necessary for one sensor node to ask for the aid of other sensor nodes in forwarding a packet to its destination, usually the base station. One important issue when designing wireless sensor network is the routing protocol that makes the best use of the severely limited resource presented by WSN, especially the energy limitation. Another important factor is providing as much security to the application as possible. In this project, an energy efficient secure node disjoint multipath routing protocol for wireless sensor networks is proposed. Here, the data packets are transmitted in a secure manner by using the digital signature crypto system. Multipath routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple paths instead of a single optimal path. The protocol guarantees loop freedom and disjointness of alternate path. We have compared the performance of this protocol with an ad hoc on-demand multipath distance vector routing protocol. To evaluate performance of proposed method, we have used parameters packet delivery ratio, energy consumption, routing overhead and throughput compare to the ad hoc on-demand multipath distance vector routing .**

***Keywords*— Wireless Sensor Network, Disjointness, Multipath ,Routing protocols, Lifetime.**

I. INTRODUCTION

Routing the sensed data from the source to sink node in a resource constrained environment in a Wireless Sensor Network (WSN) is still a challenge. There were many attempts made to route the data in the resource constrained scenarios [11]. One of the primary concerns with respect to sensor networks applications is the design and development of an energy-efficient and secure routing protocol that operates in an unattended, sometimes hostile, environment. Consuming low power is one important attribute of routing protocols for WSN. But a more useful metric for routing protocol performance is network lifetime, i.e., the protocol should ensure that connectivity in a network is maintained for as long as possible, and the energy status of the entire network should be of the same order. This is in contrast to energy optimizing protocols .Optimal path between the source and destination is selected by the routing protocols to satisfy the resource constraints such as energy, bandwidth and computation power. The routing protocols take into account the metrics like minimum hop, minimum transmission cost, high residual energy etc to route the data [2]–[5]. Many routing protocols attempt to reduce the energy usage in the nodes to increase the network lifetime. Selecting an optimal path between the source and destination and sending the data through that path may not increase the lifetime of network [6]. The energy usage in such an approach is not as efficient as that in the multi-path approaches. The multi-path routing protocols select the available possible paths between the source and destination [7]. The data is distributed among the multiple paths and the usage of energy for the data transmission is spread among the number of nodes over multiple paths. The transmission delay is reduced as portion of the data is sent in different paths. The multi-path routing protocols provide an effective load sharing mechanism among the multiple paths to satisfy the resource constraints and to meet the required Quality of Service (QoS) in the WSNs. The multipath routing increases the probability of reliable data delivery. In multi-path routing, the energy cost overhead for data retransmissions due to link failure or node failure and an alternate path construction is minimized [8].

The routing protocols suffer from a variety of security threats from the malicious nodes in the network [9], [10]. Specifically, a WSN suffers from many attacks like spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack, wormhole attack, HELLO flood attack, byzantine attack, resource depletion attack, routing table overflow, routing table poisoning, etc.

In this paper, a secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) for wireless sensor networks is proposed. It is a sink initiated proactive protocol. This protocol finds the multiple paths between the source and destination based on the rate of energy consumption and filled queue length of the node. Here, the data packets are transmitted in a secure manner by using the digital signature crypto system. This crypto system uses the MD5 hash function and RSA algorithm.

II. LITERATURE REVIEW & RELATED WORK

Marina et al [1] proposed Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. It is a source initiated, reactive (Node/link) disjoint multipath routing protocol. AOMDV extends the Ad hoc On-demand Distance Vector (AODV) protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths are computed to guarantee the network to be loop-free and disjointed. Primary design goal behind AOMDV is to provide efficient fault tolerance in the sense of faster and efficient recovery from route failures.

The route discovery is initiated by broadcasting Route REQuest (RREQ) packets to its neighbouring nodes. The source node waits for the Route REPly (RREP) packet from the destination node or intermediate nodes, which has valid path to the destination. The intermediate node on receiving the RREQ packets sets up a reverse path to the source using the previous hop of the RREQ as next hop on the reverse path. In AOMDV, route maintenance is done by means of Route ERRor (RERR) packets. When an intermediate node detects a link failure (via a link-layer feedback), it generates a RERR packet. The RERR packet propagates toward all traffic sources having a route via the failed link, and erases all broken routes on the way. A source, upon receiving the RERR initiates a new route discovery if it still needs the route. Apart from this route maintenance mechanism, AOMDV also has a timer-based mechanism to purge the stale routes. AOMDV uses very small time out values to avoid stale paths. This may limit the benefit of using multiple paths. The route discovery process has to be initiated by the sensor nodes, when it wants to send the data to sink node. The message overhead in the route discovery, and route maintenance is high in AOMDV because of its on demand nature of routing in static topology natured WSNs.

Ke Guan et al [12] proposed energy-efficient multi-path routing protocol for WSNs. It is a reactive routing protocol. In the network, every node may act as a source and a sink node. The assumption of the common base station is eliminated. The route discovery mechanism provides the multiple paths between the source and destination using shared nodes in the query tree and search tree. The number of control message packets used in the multiple route construction is high to construct a query tree and a search tree. The query messages and search messages are to be broadcasted in the network. These messages are sent from the sink and source nodes, respectively.

Marjan Radi et al [14] proposed Low-Interference Energy-Efficient Multipath Routing (LIEMRO) for WSNs. It is a source initiated event-based, reactive routing protocol. The LIEMRO model finds the multi-path between the source and destination. However, these multipaths exclude the node disjointedness property. The LIEMRO model used load balancing algorithm. The load balancing is done based on the average interference level, average residual battery and Estimated Transmit Energy (ETX) value of each path. The generation of multiple paths in LIEMRO is quite different from on-demand multipath routing protocols. Once a path between source and destination is generated and used, then it finds the second path. Usage of neighbouring control signals and separate route request packets for each path in the network demands high control overhead in the network.

Secure Cluster Based Multipath Routing Protocol (SCMRP) [17] is a proactive, hierarchical multipath secure routing protocol. The SCMRP model provides the security in routing the data using the effective key management technique like unique pair wise key distribution. The SCMRP model sends NeighBouR DETection (NBR DET) packet to construct the neighbour list in each node. Every node sends the neighbour list information to the base station. The base station generates the pair-wise key for every link in the network. These packets, neighbour list and pair-wise key received by the base station consume high energy in the resource constrained WSNs.

Secure and Energy Efficient Multi-path (SEEM) [18] routing protocol has three kinds of nodes such as sensor node, sink node and base station node. The base station plays a major role in finding multiple paths between the source and sink node. The control overhead is high in the SEEM model as it uses Neighbour Discovery (ND) packet, Neighbour Collection (NC) packet and Neighbour Collection Reply (NCR) packet in the routing protocol. The ND packet is broadcast in the network to know the neighbouring nodes of every node. Once all the nodes know their neighbouring nodes, the base station node broadcasts NC packet in order to collect the neighbour's information of each node gathered during the previous broadcasting. The sensor nodes acknowledge to the NC packet by sending the neighbour collection reply packet to the base station. The SEEM model justifies the security without using the crypto system mechanism in the routing protocol.

III. Analysis Of Problem

Routing the sensed data from the source to sink node in a resource constrained environment in a Wireless Sensor Network (WSN) is still a challenge. There were many attempts made to route the data in the resource constrained scenarios [11]. Optimal path between the source and destination is selected by the routing protocols to satisfy the resource constraints such energy, bandwidth and computation power. The routing protocols take into account the metrics like minimum hop, minimum transmission cost, high residual energy etc to route the data [2]–[5]. Many routing protocols attempt to reduce the energy usage in the nodes to increase the network lifetime. Selecting an optimal path between the source and destination and sending the data through that path may not increase the lifetime of network [6]. The energy usage in such an approach is not efficient.

The most crucial part of the WSNs is the data communication; data should reach to the sink (i.e. base station) early and as it is. Delay in data or manipulated data is useless for the user. So the essential requirement of data communication is the proper routing, till now number of routing protocols are present. These routing protocols are divided into some classes. The main class is based on network structure and protocol operation; network structure is again classified into flat, hierarchical and location based and protocol operation has negotiation, multipath, query, QoS, and coherent based, all are having its own advantages and disadvantages, but no one deals with the security. For maintaining integrity, authenticity and confidentially of the sensed data, security mechanism is must. Security also mark equally as efficiency and lifetime of the network, adding security on already implemented protocol is not feasible.

The routing protocols suffer from a variety of security threats from the malicious nodes in the network [9], [10]. Specifically, a WSN suffers from many attacks like spoofing or altering the route information, selective forwarding, sinkhole attack, sybil attack, wormhole attack, HELLO flood attack, byzantine attack, resource depletion attack, routing table overflow, routing table poisoning, etc.

IV. PROPOSED WORK AND OBJECTIVES

In this paper, a secure Energy Efficient Node Disjoint Multipath Routing Protocol is proposed. It is a sink initiated proactive protocol. This protocol finds the multiple paths between the source and destination based on the rate of energy consumption and filled queue length of the node.

A. Assumption

The following assumptions are made for this work:

1) N is the number of identical wireless sensor nodes that are deployed randomly in the phenomenon with a single sink node. All the sensor nodes send the sensed information to the destination (sink node) over the multiple hops.
2) The WSN is assumed to be an undirected graph G (V, E), where, V is the set of nodes and E is the edge set such that E ⊂ V X V. The link (i, j) € E, if nodes i and j can communicate with each other. N_i is the set of all nodes that can be reached in one hop from node i .
3) Each sensor node has a fixed transmission range R. Multiple paths are available between the source and sink node in the network. The source node selects the node-disjoint paths between the source and destination to route the sensed data to the sink node.
4) Every node has a unique private key and a public key.
5) Common hash function is used by all nodes in the network.

B. Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP)

Let us consider that, WSN is consist of number of stages St_i , i = 1, 2,…,i. The node is at stage zero i.e St_0 and the nodes which can directly communicate with sink node are at stage one St_1. The nodes which are two hopes away from the sink node are at stage two, St_2 and so on. The node at stage St_i can communicate only with node at same stage, St_i or node at next stage i.e St_{i+1} but it cannot communicate with the node at previous stage, St_{i-1} which prevents the loop formation within Wireless sensor networks.

Also we assume that, initially the hop count of each node except the sink node is high and the residual energy of each node within network is greater than that of the threshold energy. The working of EENDMRP consist of two phases –

1) Route Construction Phase
2) Data Transmission Phase

1) Route Construction Phase :

In EENDMRP, the route construction phase is initiated by sink node (as it is a sink initiated protocol) by broadcasting the Route Construction (RCON) packet to its neighboring nodes. The format for of RCON packet is shown in Fig 1.

Packet Type	Hop Count	Forward ID	Threshold Energy	Route	Forwarder's Public Key
1 Byte	2 Bytes	2 Bytes	4 Bytes	2 Bytes	4 Bytes

Fig . 1 Format of route construction (RCON) packet.

This packet consist of packet type to know whether the packet is control packet or data packet, beacon hop count which indicate the number of hops away from the sink, beacon source i.e original sender of beacon, node threshold energy level, Path (packet traversed from sink to node) field and forwarder node's public key. The format of the routing table is shown in Fig. 2.

NODE ID	Hop Count	Node Cost	Residual Energy	Node Disjoint Paths	Neighboring node's Public Key

Fig. 2 Format of node routing table.

If there is no route to the sink via the node that received RCON packet, then that node processes the RCON packet. If the route to sink from that node is already available in the node's routing table then it checks the packet's hop count value. If packet hop count is smaller than node's hop count value and its residual energy is above the threshold energy value, then RCON is processed; otherwise the packet is dropped. The node that receives the RCON packet, updates the RCON packet. The updated RCON with hop count incremented by one, updates the forward node id and appends its node id to the path. The node which receives the route construction packet updates its routing table information such as node's hop count and route to the sink node. Similarly, all the nodes in the network receive the route construction packet and update their routing table. This process is repeated until all the nodes in the network generate their routing table.

This protocol finds the route on the basis of metric like hop count and filled queue length. Now let us illustrate this phase with the help of one example. Consider the WSN in Fig 3.

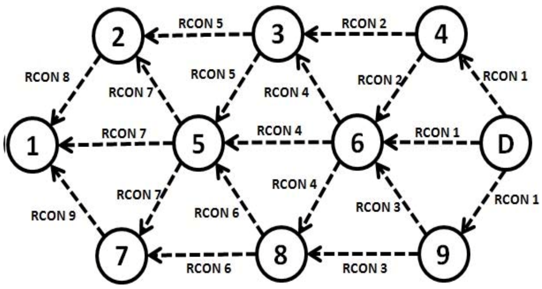

Fig. 3. Route construction phase in EENDMRP.

Suppose D is the sink node then it broadcasts RCON packet to its neighboring node i.e node 4,6, and 9. After receiving this packet, node 4 first check whether its hop count is greater than that of the hop count in RCON packet and residual energy at node 4 is greater than threshold energy. If both conditions get satisfied then and only then node 4 processes that packet and updates its routing table otherwise it update only its public key and forward it towards its neighboring nodes and so on. Each node do the same process. And this process will be continued until all the nodes within the network generate their routing table.

2) Data Transmission Phase:

In this phase, the source node chooses one of the primary path from previously constructed multiple path for sending the data from source node to sink node. The primary path is chosen on the basis of maximum Path Cost (PC) and the path cost is calculated on the basis of various node parameters like energy consumption, filled queue length and residual energy at particular node. For calculating the path cost , first we calculate the node cost f each node. Suppose if we want to calculate the node cost of j^{th} node then we calculate the energy required for sending the data, filled queue length in the buffer of j^{th} node and residual energy at j^{th} node. Minimum is the node cost , less is the probability of data transfer through thst node. Likewise every node in the path finds its cost. If the j^{th} node has minimum cost then the path cost of that whole path is the node cost of the j^{th} node. Similarly, if all the path costs PC_i i = 1, 2,…., k are evaluated then the primary path PP is chosen as the path which has the maximum path cost. This is to say that the path which can handle maximum data traffic and is a more reliable path among the node disjoint paths. Let k be the number of multiple paths between the j^{th} node and sink and m be the number of nodes in the path Pi, REC_{old} is the previous rate of energy consumption, REC_{new} is the current rate of energy consumption and REC_j is the average rate of energy consumption of the j^{th} node. REC_j is evaluated using the well-known Exponential Weighted Moving Average (EWMA) technique

$$REC_j = \alpha * REC_{old} + (1 - \alpha) * REC_{new} \qquad (1)$$

where, the coefficient α € (0, 1) represents the degree of weighting decrease and is a constant smoothing factor. To better reflect the current condition of energy expenditure of nodes, this work sets α as 0.3 as in [26]. Let FQL j be the filled queue length of the j^{th} node, RE_j be the residual energy of the j^{th} node and NC_j be the node cost of the j^{th} node.

Then

$$NC_j = (RE_j / REC_j) * FQL_j \qquad (2)$$

The path cost PC_i of the path P_i is

$$PC_i = \min\{NC_j \text{ where, } j \in m\}. \qquad (3)$$

The primary path PP among the multiple paths between source and sink is selected as

$$PP = \max\{PC_i \text{ where, } i \in k\}. \qquad (4)$$

C. Security in EENDMRP

We have designed the security in EENDMRP using the asymmetric (public) key crypto system. To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It may be used to provide both secrecy and digital signatures. Its security is based on the intractability of the integer factorization problem [27].The major advantage of RSA is that it does not increase the size of the message. It may be used to provide privacy and authentication over communication links through digital signatures [28]. In the past, the constraints of sensor networks have fostered a belief in some researchers that many Internet level security techniques are heavyweight for sensor networks and that new alternatives must be developed. This opinion has led to interesting new research. Westoff et al [28] demonstrate that with careful design, the widely used RSA public key crypto system can be deployed on even the most resource constrained sensor network devices. The verification time of RSA is found to be more than 30 times faster than ECDSA. The signature generation is measured to be 8 times slower than ECDSA. Wander et al [29] suggest that an optimal choice of a digital signature depends on the demand of the application. The RSA is well suited for certificate based systems that require few signature generation and large number (thousands) of verifications. Westoff et al [28] also state that, when the number of hops between source and sink node is more than 5, RSA performs better than ECDSA in CPU execution cost per packet. If, the number of hops is less than 5, then ECDSA is better than RSA.

Wander et al [29] presented the interesting results that the power required to transmit 1 bit is equivalent to roughly 2090 clock cycles of execution on the microcontroller alone. In this work the focus is on providing the security in routing protocol with concern to privacy, authentication and non-repudiation of the data in the network. The security in EENDMRP will be analysed using RSA Public key crypto system. Initially it is assumed that all the sensor nodes have their unique public key during its deployment in the phenomena. During the route construction phase, the sink broadcasts RCON packets to its neighbouring nodes. The neighbouring nodes receive the RCON packet. A neighbouring node updates RCON packet with its public key. It rebroadcast the RCON packet to its neighbouring nodes. Similarly all the nodes in the network update their routing table with their neighbouring node's public key. Here, the nodes receive the RCON packet even from the St_{i+1} stage nodes. A node updates its routing table with the St_{i+1} stage node's public key and discards the packet without forwarding to its neighbouring nodes. Here, the objective is that every node should know public key of its neighbouring node i.e., which are reachable in one hop. In the data transmission phase, the source node selects the node-disjoint paths to the sink node and sends the data traffic through it. The source node picks M amount of data to send through the node-disjoint primary path to the sink. The MD5 hash function H will be used to create message digest H(M) at the source node. The source node will generate the digital signature d_{sign} = (H (M))d mod n by encrypting the message digest H(M) with its private key d where, n = p * q, p and q are random prime numbers with p ≠ q. The source node forwards d_{sign} with data M, (d_{sign}, M) to its neighbouring node through the path it takes to reach sink. A neighbouring node on reception of (d_{sign}, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of design mod n with message digest H(M). The d^e_{sign} mod n is key (e, n) using the formula, decrypted using sender's public key.

$$d^e_{sign} \bmod n = ((H(M))^d \bmod n)^e \bmod n$$
$$= (H(M))^{ea} \bmod n \qquad (5)$$

By applying Little Fermat's and Chinese Remainder Theorem to Equation (5), it can be shown that

$$d^e_{sign} \bmod n = H(M) \qquad (6)$$

If the generated H(M) by the receiver and the decrypted H(M) of digital signature d_{sign} is equal, then the receiver accepts the data; otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. This process is repeated in every hop of the node disjoint path between source and destination. The proposed public key crypto system provides authentication, integrity and non-repudiation in the wireless sensor network.

1) Correctness of RSA Public Key Crypto System in EENDMRP

The confirmation of the data source in the EENDMRP at the sink node is shown in the following steps. We know that, the digital signature d_{sign} is generated using $d_{sign} = ((H(M))d \bmod n)$ and decrypted using source public key e

$$H(M) = (d^e(\bmod n)) \quad (7)$$
$$= ((H(M)d)^e(\bmod n))$$
$$= (H(M))^{ed} \bmod n$$
$$= (H(M))^{1+k(p-1)(q-1)} \bmod n$$
$$H(M) = (H(M)).(H(M))^{k(p-1)(q-1)} \bmod n$$

using, $ed \equiv 1 \bmod (\phi(n))$ and replacing $(\phi(n))$ with $ed = 1+k(p-1)(q-1)$. The Little Fermat's theorem states that if $a > 1$ be an integer and p is any prime with $(a, p) = 1$ then $a^{p-1} \equiv 1 \bmod p$. Hence

$$H(M)^{p-1} \bmod p = 1. \quad (8)$$

Similarly, $H(M)^{q-1} \bmod q = 1$. Consider

$$H(M)[H(M)]^{k(p-1)(q-1)}(\bmod p) \quad (9)$$

on rearranging (9) is equivalent to $H(M)[H(M)(p-1)(\bmod p)]^{k(q-1)}$
using (8) it is equivalent to H(M). Similarly

$$H(M)[H(M)]^{k(p-1)(q-1)}(\bmod q) = H(M). \quad (10)$$

Chinese Remainder Theorem states that, if $a \equiv b(\bmod p)$, and $a \equiv b(\bmod q)$ then, $a \equiv b(\bmod p.q)$ using (9) and (10) together with Chinese Remainder Theorem, it can be shown that

$$H(M)[H(M)]^{k(p-1)(q-1)} = H(M)(\bmod p.q)$$

from Equation (7)

$$H(M) \equiv H(M)(\bmod n) \text{ since, } n = pq$$

Hence it confirms that the data received at the sink node is the data sent from last hop of the path.

V. Result And Discussion

The EENDMRP model is implemented using Network Simulator 2.34 The simulation parameters are 700 × 700 sq.m area, 1 to 20 numbers of nodes with grid topology, 802_15 MAC layer and two ray ground radio propagation models. The EENDMRP model is compared with the AOMDV model from different perspectives such as packet delivery fraction, end-to-end delay, normalized routing overhead, energy consumption and throughput.
The network simulator set up is shown in Table I

TABLE I.
SIMULATION PARAMETER

Simulator	Ns-2 (Version 2.34)
Simulation Time	300 (s)
Number of mobile nodes	20
Routing Protocol	AOMDV
Traffic	CBR
Transport Protocol	UDP
Packet Size	512 Bytes

A) Comparison of EENDMRP and AOMDV Protocol in terms of Packet Delivery Fraction.

Packet Delivery Fraction is the ratio of the data packets delivered to the destination to those generated by constant bit rate sources. Fig 4 shows the PDF of EENDMRP and AOMDV varying the simulation time. From the figure we can see that the number of dropped packets in EENDMRP is less than that in AOMDV protocol.

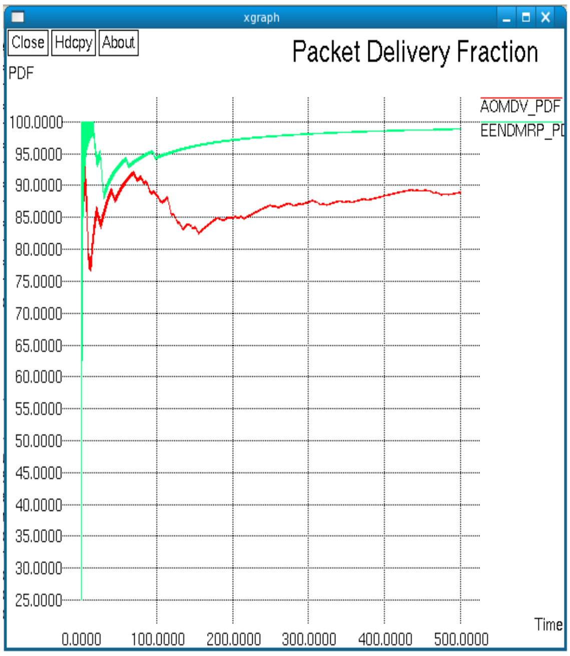

Fig 4. Variation of Packet Delivery Fraction with Simulation time

B)Comparison of EENDMRP and AOMDV Protocol in terms of Normalized Routing Load.

Normalized Routing Load is the number of routing packets transmitted per data packet delivered at the destination. Each hop wise transmission of routing packet is counted as one transmission.
Fig 5 shows the Normalized Routing Load in EENDMRP and AOMDV varying the simulation time. From the figure we can see that Normalized Routing Load in EENDMRP is less than that in AOMDV protocol since the number of control messages used in constructing the multiple path is less in EENDMRP as compared to AOMDV protocol.

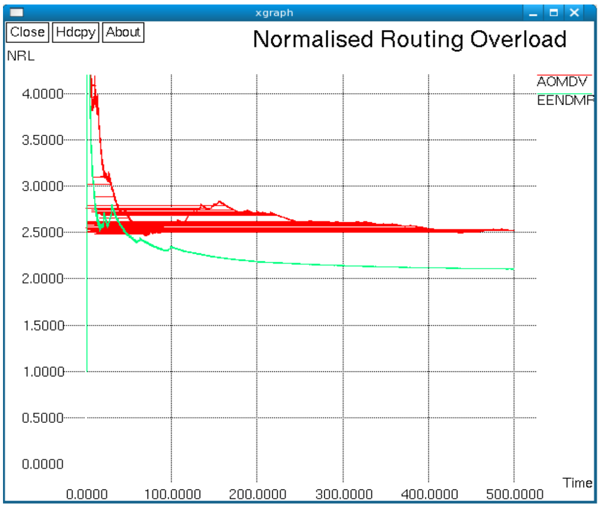

Fig 5. Variation of Normalized Routing Load with Simulation time

*C) Comparison of EENDMRP and AOMDV Protocol in terms of Energy Consumption***.**

Average energy spent by the sensor nodes in the network is one of the important metrics to evaluate the energy efficiency of routing protocol.

Fig 6 shows the Average energy remaining at each node in EENDMRP and AOMDV varying the number of nodes. From the figure we can see that Average energy remaining at each node in EENDMRP is much more than that in AOMDV protocol.

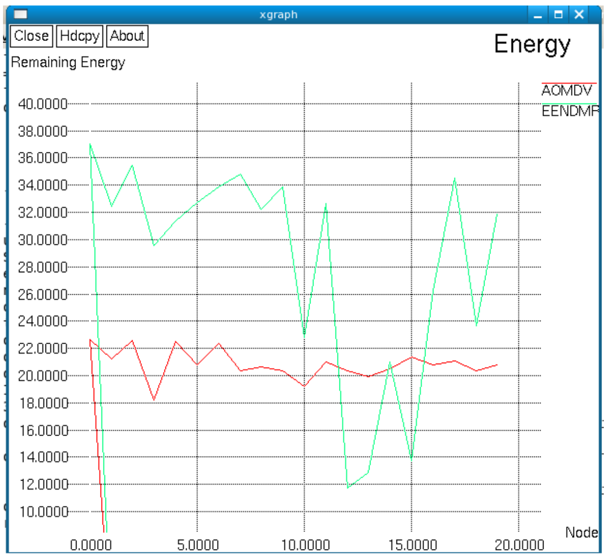

Fig 6. Variation of Average energy remaining at each node with number of nodes

D) Comparison of EENDMRP and AOMDV Protocol in terms of Throughput.

Network throughput is the rate of successful message delivery over a communication channel. Throughput is the number of messages successfully delivered per unit time.

Fig 7 shows the Throughput in EENDMRP and AOMDV varying the simulation time. From the figure we can see that Throughput in EENDMRP is more than that in AOMDV protocol .

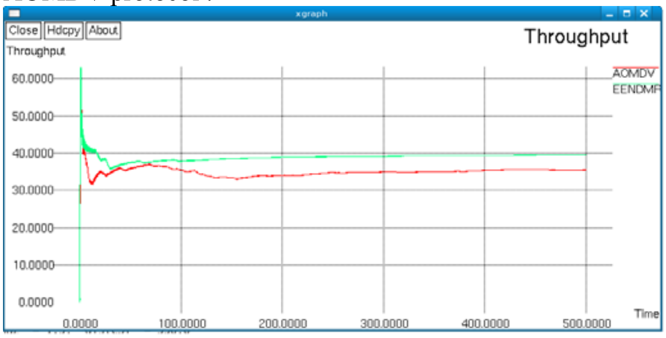

Fig 7. Variation of Throughput with simulation time

VI. Application

Along with the rapid advances in electronics and wireless communications are the broad applications of Wireless Sensor Networks (WSN). WSN is formed by densely and usually randomly deploying large number of sensor nodes either inside or very close to the phenomenon that is being monitored. Thus, the applications can be both military and civilian, such as environment monitor, wild animals track, homeland security, etc.

Sensor networks have many applications from the field of medical to battle field and from the homeland security to earthquake monitoring.

This section describes some of the most prevalent applications for wireless sensor networks.

A) Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines. Area monitoring is most important part.

B) Health care monitoring

The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.

1) Air pollution monitoring

Wireless sensor networks have been deployed in several cities (Stockholm, London and Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

2) Forest fire detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

3) Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

4) Water quality monitoring

Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.[5]

5) Natural disaster prevention

Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.

C) Industrial monitoring

1) Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality.[6] In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

2) Data logging

Wireless sensor networks are also used for the collection of data for monitoring of environmental information, this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.

3) Water/Waste water monitoring

Monitoring the quality and level of water includes many activities such as checking the quality of underground or surface water and ensuring a country's water infrastructure for the benefit of both human and animal.

4) Structural Health Monitoring

Wireless sensor networks can be used to monitor the condition of civil infrastructure and related geo-physical processes close to real time, and over long periods through data logging, using appropriately interfaced sensors. Resultant data streams can be dynamically, or post (i.e. offline), analyzed to determine if potentially dangerous situations are arising, allowing for safety measures to be taken; including informing advance warning systems, and scheduling preventative maintenance.

VII. CONCLUSION

Wireless Sensor Network has been active research based area over the past few years, due to their application in military and civilian communication In this project, we proposed the secure Energy Efficient Node Disjoint Multipath routing Protocol which find outs loop free , disjoint multiple path from sink node to source node to increase the lifetime of the wireless sensor network. The effective routing metrics like, buffer utilization, residual energy and the drain rate are used in selecting the primary path in the energy efficient node-disjoint multipath routing protocol. From the experimental result, we can say that EENDMRP protocol provides the better and efficient result in terms of various metric values such as packet delivery ratio, energy consumption, routing overhead and throughput than AOMDV protocol. The proposed protocol provides the security using digital signature, which is generated by using the MD5 hash function and RSA algorithm. The security ensures the correctness of data, nonrepudiation and authentication. The proposed protocol defends data tampered or altered routing, selective forwarding, sink hole and byzantine attacks.

VIII. FUTURE WORK

In this paper EENDMRP is limited to physical data routing and multimedia data routing is not taken into consideration. We can design a new metric measuring energy and QoS with link reliability.

Future work will involved some new additional features or parameters using which there is a much more increment in the performance metrics of the network as well as try to avoid the different attacks which occur on the network, with the use of different network security algorithms.

REFERENCES

[1] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. Int. Conf. Netw. Protocols*, 2001, pp. 14–22.

[2] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris, "Toward resilient routing in wireless sensor networks: Gradient-based routing in focus," in *Proc. 4th Int. Conf. Sensor Technol. Appl.*, 2010, pp. 478–483.

[3] H. Zhang and H. Shen, "Energy-efficient beaconless geographic routing in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 881–896, Jun. 2010.

[4] M.-C. Zheng, D.-F. Zhang, and J. Luo, "Minimum hop routing wireless sensor networks based on ensuring of data link reliability," in *Proc. Int. Conf. Mobile Ad-Hoc Sensor Netw.*, 2009, pp. 212–217.

[5] L. Cheng, S. K. Das, J. Cao, C. Chen, and M. Jian, "Distributed minimum transmission multicast routing protocol for wireless

sensor networks," in *Proc. Int. Conf. Parallel Process.*, 2010, pp. 188–197.

[6] T. Hou, Y. Jianping, and S. F. Midkiff, "Maximizing the lifetime of wireless sensor networks through optimal single-session flow routing," *IEEE Trans. Moible Comput.*, vol. 5, no. 9, pp. 1255–1266, Sep. 2006.

[7] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy- effcient multipath routing in wireless sensor networks," *Mobile Comput. Commun. Rev.*, vol. 1, no. 2, pp. 1–13, 2002.

[8] Y. Ganjali and A. Keshavarzian, "Load balancing in ad hoc networks: Single-path routing versus multi-path routing," in *Proc. INFOCOM*, 2004, pp. 1120–1125.

[9] Y. K. Tan, *Sustainable Wireless Sensor Networks*. Rijeka, Croatia: Intech Publishers, Dec. 2010, ch. 12, pp. 279–309.[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. IEEE Int. Workshop Sensor Netw. Protocols Appl.*, May 2003, pp. 113–127.

[11] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *Comput. Netw.*,vol. 11, no. 6, pp. 6–28, 2004.

[12] K. Guan and L.-M. He, "A novel energy-efficient multi-path routing protocol for wireless sensor networks," in *Proc. Int. Conf. Commun. Mobile Comput.*, Apr. 2010, pp. 214–218.

[13] M. Radi, "LIEMR: A Low-interference energy-efficient multipath routing protocol for improving QoS in event-based wireless sensor networks," in *Proc. Int. Conf. Sensor Technol. Appl.*, 2010, pp. 551–557.

[14] M. Bheemalingaiah, M. M. Naidu, D. S. Rao, and G. Varaprasad, "Power-aware node-disjoint multipath source routing with low overhead in MANET," *Int. J. Mobile Netw. Design Innovat.*, vol. 3 no. 1, pp. 33–45, 2009.

[15] D. B. Johnson, D. A. Maltz, and J. Broch, "Dynamic source routing protocol for mobile ad hoc networks," in *Proc. IETF Internet Draft*, 2004, pp. 139–172.

[16] S. Kumar and S. Jena, "SCMRP: Secure cluster based multipath routing protocol for wireless sensor networks," in *Proc. 6th Int. Conf. Wireless Commun. Sensor Netw,* 2010 pp.1–6.

[17] N. Nasser and Y. Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 11, pp. 2401–2412, 2007.

[18] A. Juels. (2011). *Cryptographic Tools* [Online]. Available: http://www. rsa.com/rsalabs/node.asp

[19] A. Wadaa, S. Olariu, and L. Wilson, "Scalable cryptographic key management in wireless sensor networks," in *Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops*, 2004, pp. 1–7.

[20] A. K. Das and D. Giri. (2011). An identity based key management scheme in wireless sensor networks. *CoRR* [Online]. Available: http://arxiv.org/pdf/1103.4676.pdf

[21] Y. K. Jain and V. Jain, "An efficient key management scheme for wireless network," *Int. J. Sci. Eng. Res.*, vol. 2, no. 2, pp. 1–7, 2011.

[22] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, pp. 1–11, Dec. 2011.

[23] C. Xu and Y. Ge, "The public key encryption to improve the security on wireless sensor networks," in *Proc.2nd Int. Conf. Inf. Comput. Sci.*, 2009, pp. 11–15.

[24] X. Huang, D. Sharma, M. Aseeri, and S. Almorqi, "Secure wireless sensor networks with dynamic window for elliptic curve cryptography," in *Proc. Electron., Commun. Photon. Conf.*, 2011, pp. 1–5.

[25] D. Kim, J. J. Garcia-Luna-Aceves, and K. Obraczka, "Routing mechanisms for mobile ad hoc networks based on the energy drain rate," *IEEE Trans. Mobile Comput.*, vol. 2, no 2, pp. 1–6, Apr.–Jun. 2003.

[26] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Sensor netwok with public key technology," in *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw.*, 2004, pp. 59–64.[27] C. D. Westhoff, B. Lamparter, and A. Weimerskirch, "On digital signatures in ad- hoc networks," *J. Eur Trans. Telecom*, vol. 16, no. 5, pp. 411–425, 2005.

[28] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis public-key cryptography for wireless sensor networks," in *Proc. 3rd IEEE Int.Conf. Pervasive Comput. Commun.*, 2005, pp. 324–328.