Volume 4, No. 4, March-April 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Energy Aware Multi-hop Routing Protocol for Wireless Sensor Networks

V.Chandrasekaran*
Asst.Professor (Sr.Gr), Department of ECE,
Velalar College of Engineering and Technology,
Erode-638 012
mail.vcresearch@gmail.com

K.Lalitha
Asst.Professor, Department of IT,
Kongu Engineering College,
Erode-638 052
klalitha@kongu.ac.in

S.Anitha
Asst.Professor, Department of IT,
Kongu Engineering College, Erode-638 052
anithame@kongu.ac.in

Abstract: In resource constraint Wireless Sensor Networks, reducing the energy consumption is a critical task. The objective of energy aware routing protocol is to increase the operational lifetime of the wireless sensor networks. Multiple-path transmission is one of the methods for ensuring QoS routing in both wired and wireless environment. Multi-hop routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple routes instead of a single optimal routing. Secured data transmission is also an important research issue in the wireless sensor networks. In this paper, a Secure Energy Aware Multi-path and Multi-hop Routing Protocol (SEAMMRP) for wireless sensor networks is proposed. The parameters considered along with routing are energy consumption, end-to-end delay, packet delivery ratio and thus improving the Quality of Service (QoS). Digital Signature system is used for secure data transmission. This protocol is compared with the Ad hoc On-demand Multipath Distance Vector (AOMDV) Routing protocol and EENDMRP protocol using Network Simulator(NS-2) and it shows better results in the parameters considered.

Keywords: -Multi-path Routing, Multi-hop Routing Protocol, Digital Signature, AOMDV Protocol, Quality of Service

I. INTRODUCTION

In Wireless Sensor Network (WSN), routing the sensed data from the source to the sink node in a resource scarce environment is still a challenging issue. In such scenarios, many attempts are made to route the data [1]. To minimize such resources like energy, bandwidth and computation power, optimal path is selected to transfer data from the source to destination. Metrics like minimum hop count and transmission cost, high residual energy etc are taken into account to route the data while choosing the appropriate routing protocol [2]–[3]. Many routing protocols improve the longevity of the network attempt in order to reduce the energy spent. During the past few decades, the development of wireless sensor networks (WSNs) become a promising area as the embedded microprocessors, low-power analog and digital electronics, and radio communications advances. WSN consist of a large number of battery-operated sensor nodes SNs scattered in a random manner. In WSN, sensor nodes collect data from surrounding areas and transmit it to sink nodes for further processing. Different portions of data are transmitted in different paths to reduce transmission delay. To accomplish this, load balancing multipath routing mechanism is used to satisfy the Quality of Service (QoS) in the WSNs. Thus probability of reliable data delivery is improved and energy overhead due to link or node failure is minimized with this multipath routing [4].

Different classes of routing mechanisms that allow multiple paths established between the source and the destination is described using Multipath routing. 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 affect the WSNs [5]-[6].

In this paper, a Secure Energy Aware Multi-path and Multi –hop routing protocol (SEAMMRP) is proposed. It is a proactive protocol with sink initialization. It addresses the attacks like spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack, wormhole attack, HELLO flood attack, byzantine attack with the help of Digital Signature on the hash algorithm and cryptographic techniques. The Hash function and the RSA algorithm are used to implement the digital signature in SEAMMRP protocol.

The rest of the paper is organized as follows: In Section II, review of related work is discussed. In Section III, design architecture of the Secure Energy Aware Multi-path and Multi–hop routing protocol (SEAMMRP) is presented. In Section IV, Cryptographic techniques for implementing the digital signature are given. The implementation of Secure Energy Aware Multi-path and Multi –hop routing protocol (SEAMMRP) is presented in Section V. Section VI deals with the comparison of AOMDV protocol with SEAMMRP protocol. Section VII is concluded with final results and future enhancements.

II. REVIEW OF RELATED WORKS

The central part of the AOMDV protocol lies in confirming the loop-free and disjoint paths for efficient transmission using flood-based route discovery [7].To accomplish loop-free and disjointness properties, AOMDV updates route rules at each local node.

In CBMPR (cluster-based multi-path routing), cluster-based routing and multi-path routing are combined efficiently. By using this cluster network, multiple paths are found and thus forming the independent paths. Fig 1 shows an example of choosing routing paths through different clusters among multiple paths causing less interference.

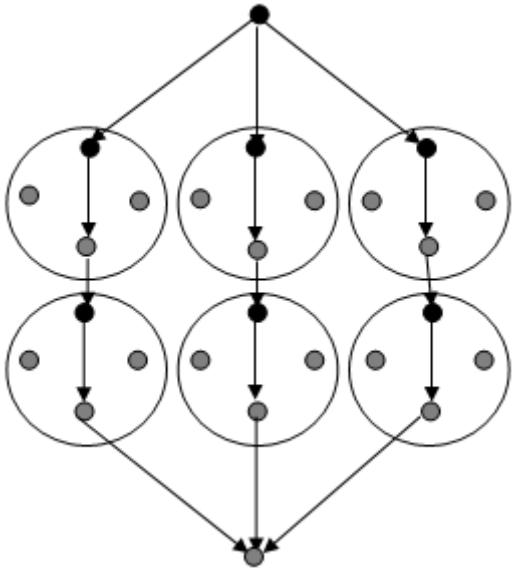

Figure.1 Multiple paths established with CBMPR

The main advantages of CBMPR over traditional multi path routing is less interference and simplicity. In this proposed cluster level hop-by-hop routing approach, each path passes through the heads of clusters [8]. In [9], an energy-aware QoS routing mechanism for wireless sensor networks is presented. The proposed protocol considers end-to-end delay only and extends the routing approach. The incoming packets are segmented into fixed sized sub-packets and reassembled for transmission across the multiple paths. In each sub-packet, error correction codes are appended to transmit the reliable data and reducing path failures. The important portion of data is transmitted without delay and increased energy consumption for retransmission is ensured in the segmented sub-packets. Sub-packets received by the sink node reassembled to generate original packet. Based on the results of the cost function calculated in each link, delay-constrained path having minimum cost is chosen. Recursively the procedure is repeated starting with higher cost value until the path with reduced delay and maximum throughput is found.

In multipath routing approach, the sensing field consists of sensor nodes scattered in a random manner. The network is assumed to be placed in an interesting area with unique ID for each node and all are actively participating in packet transmission and reception. A priori, fixed lifetime and identifiers of each node is also assumed. Optimal traffic flow in each multiple paths is done by multipath routing protocol adaptively [10].

An Energy Efficient Multi path routing protocol proposed in [11] discover multiple node-disjoint paths between the sink and sources using distributed, scalable and localized multipath search algorithm. Distribution of traffic over multiple paths is also discovered using load balancing algorithm. Based on their cost, this algorithm allocates traffic over multiple paths by the sink of which cost depends on the energy levels and hop distances of nodes along each path. While comparing our proposed protocol with the existing energy-aware routing protocols, the simulation experiment shows that the proposed protocol outperforms in increased energy efficiency, reduced delay and control overhead over traditional protocols.

For real-time data, minimum cost with reduced delay is found by several energy-aware QoS protocols. Various Communication parameters such as the maximum energy in the nodes, energy transmitted and error rate are defined by the cost of the link. By adjusting the service rate for both real- and non real-time traffic, throughput of the non real-time data can be maximized by the cost of the link. A class-based queuing model is used to provide both real- time and non- real time QoS simultaneously. The first demerit of this approach is that it does not provide importance to the real-time data for different end-to-end delay requirements compared to non-real time traffic. The second demerit is that the proposed scheme is not suited for several other delays from MAC-related channel or queuing delay of packets at intermediate nodes [12]. In this protocol, network delay calculated is not acceptable for different other QoS protocols which conserves energy but still there is no scheme that provide the optimum solution.

The amount of data that the nodes sense is significantly less than the data they transmit in multi-hop routing protocol as the Sink Connectivity Area (SCA) contains less number of nodes than the number outside the SCA and thus results in increased energy consumption.[13] proposed hybrid algorithms such as hierarchical and flat multi-hop routing to conserve the energy consumption by restricting the influx of data coming into the SCA, and ensures efficient data relay inside the SCA respectively. The number of dropped packets in the EENDMRP model is less than that in the AOMDV model. The EENDMRP model is a proactive multipath routing table and routes are readily available to the sink node. In route construction phase, the node receives the route construction packet only when its hop count is greater than the Route Construction packet's hop count.

The AOMDV model is a reactive multi-path routing protocol. When the source node gets data to send, the route discovery is done from the source node to the sink. The end-to-end delay is more in the AOMDV model because of its reactive nature. In the AOMDV model, the number of control messages used in constructing multiple paths is high as compared to the EENDMRP model. The average energy spent by each node in the EENDMRP model is less as compared to the AOMDV model. The EENDMRP model is a proactive protocol. In the route construction phase, all the nodes in the network generate their routing tables and find the path to the sink. In the AOMDV model, route to sink is generated only when it is required. EENDMRP performs better than AOMDV

in above said parameters but limited to textual data routing. Mutimedia data routing and energy and QoS measurement with link reliability is not taken into consideration [1].

III. NODE DESIGN ARCHITECTURE

The following assumptions are made for the construction of Wireless sensor network scenario:

a. The sensors in the wireless sensor network are distributed as per a homogeneous spatial Poisson process of intensity in 2-dimensional space.
b. All nodes are homogenous and have the same strength.
c. Variable n is the sensor node and N is the group of sensor nodes that are randomly deployed in the environment.
d. Multiple sink nodes are placed to receive the sensed information from various source nodes over the multiple hops for energy efficiency.
e. Cryptographic techniques are used to provide secure data transmission. So every sensor node has a unique private key and a public key known for both sender and receiver.
f. The transmission range is fixed for each same power level sensor nodes. Multiple paths are available between the sink node and source node in the network. The sink node selects node disjoint paths to route the sensed data to its source nodes.
g. Secure Hash Algorithm (SHA-2) is used by all nodes for encryption of a data in the network.

IV. CRYPTANALYSIS IN WIRELESS SENSOR NETWORKS

Public key encryption - Public key encryption uses a combination of a private key and a public key. The private key is known only to the user while the public key is given by the users to any others that want to communicate securely with it. To decode an encrypted message, computer must use the public key provided by the originating computer and its own private key. The key is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value.

To implement public key encryption on a large scale, such as a secure Web server, requires a different approach. This is where digital certificates come in. A digital certificate is essentially a bit of information that informs the Web server is trusted by an independent source known as a Certificate Authority. The Certificate Authority acts as the middleman that both computers trust. It confirms that each computer is in fact who they say they are and then provides the public keys of each computer to the other.

The Digital Signature Standard (DSS) is based on a type of public key encryption method that uses the Digital Signature Algorithm (DSA). The DSA algorithm consists of a private key that only the originator of the document (signer) knows and a public key.

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value and is also commonly used to check data integrity. An MD5 hash is expressed as a hexadecimal number, 32 digits long. However, it has been shown that MD5 is not collision resistant and hence MD5 is not suitable for applications like SSL certificates or digital signatures.

To avoid collision and to provide a highly secure data transmission, an efficient algorithm is required. Secure Hash Algorithm (SHA-2) is chosen that provides better security.

Cryptographic hash functions, also known as secure hash algorithms, take an arbitrary length string and return a fixed-length hash value. Strong cryptographic hash functions make it easy to compute the hash value from an input string but very difficult to find a message that results in a particular hash value, modify a message without changing its hash value, or find two messages that hash to the same value. Digital signature algorithms rely on cryptographic hash functions. To sign a message, the signer first computes the hash value of the message, then encrypts the hash value with his or her private key. To verify a message, the verifier decrypts the signature with the signer's public key and verifies that the decrypted value matches the message hash. A Public Key Infrastructure (PKI) uses digital signatures when creating and verifying certificates.

V. SECURE ENERGY AWARE MULTI-PATH AND MULTI-HOP ROUTING PROTOCOL (SEAMMRP)

The wireless sensor networks (WSN) is depicted as an undirected graph G(V,E), as shown in Figure 2, where V is the set of all sensor nodes and all sink nodes, E is the set of all links.

$$V = V_{sink} \cup V_{source}, E = \{(n1, n2) \mid n1, n2 \square V\}$$

Every sensor's initial energy is E_{init} and its residual energy is E_{RES}. The path is defined as $\{V_1, V_2\ldots, V_{n1}, V_{n2}\ldots, S\}$, V_{n1}, $V_{n2} \in V_{source}$, $S \in V_{sink}$; the cost is defined as the cost of one link $< V_{ni1}, V_{ni2} >$.

$$Cost_{n1n2} = \alpha * dis^{2} + \beta \text{ ---------- (1)}$$

Now we define the path cost as follows:

$$pathcost = \Sigma cost_{n1n2} * E_{RES}^{\gamma} \text{ ---- (2)}$$

where α=energy/bit consumed by the transmitter electronics
β=energy/bit consumed by the transmitting and receiving signal operation overhead for amplifying
dis=distance between two sensor nodes and
γ=coefficient of residual energy and it is a non-zero negative value.

From (1) and (2), if the transmitting distance or overhead is higher, the transmission cost increases. Increasing the hop count between the sink and source nodes will automatically increases the path cost. Other factors that influences the increase in path cost is decrease in residual energy and the excessive use of the path.

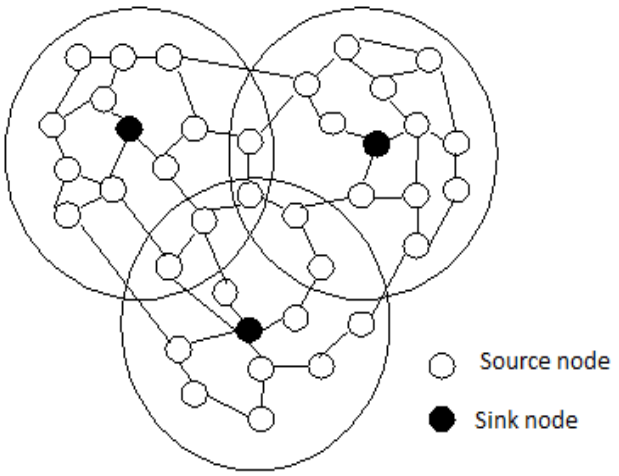

Figure.2 Clustered multiple sink sensor network with disjoint nodes

The node-disjoint routing play an important role in reducing the path cost and the following algorithm shows how this node disjoint is achieved effectively.

ALGORITHM:

To find a maximal set of vertex disjoint paths from sink node to the source nodes

Steps:

a. Make an adjacency matrix.
b. Count the number of arcs or edges connected to any vertex.
c. Traverse the list if the no. of edges in any particular node is zero.
d. Count that node; the final outcome will contain all the nodes that are disjoint.

The following pseudo code explains the above algorithm steps:

Suppose that the number of nodes in the graph is constant that is edges may be added or deleted but nodes may not.

```
# define MAXNODES 50
Struct node {
};
Struct edge {
int adj ;
};
Struct graph {
Struct node nodes [MAXNODES];
Struct edge edges [MAXNODES] [MAXNODES];
};
Struct graph G;
int adj [MAXNODES] [MAXNODES];
void join (int adj [ ] [MAXNODES], int node1, int node2)
{
adj [node1] [node2] = TRUE;
}
int adjacent (int adj [ ] [MAXNODES], int node1, int node2)
{
return ((adj[node1] [node2]==TRUE)?TRUE:FALSE);
}
```

Each node of the graph is represented by an integer between 0 and MAXNODES-1 and the array field nodes represent the appropriate information assigned to each node. The array field edge is a two dimensional array representing every possible ordered pair of nodes. The node disjoint path routing is constructed and it is clearly given in the following flowchart:

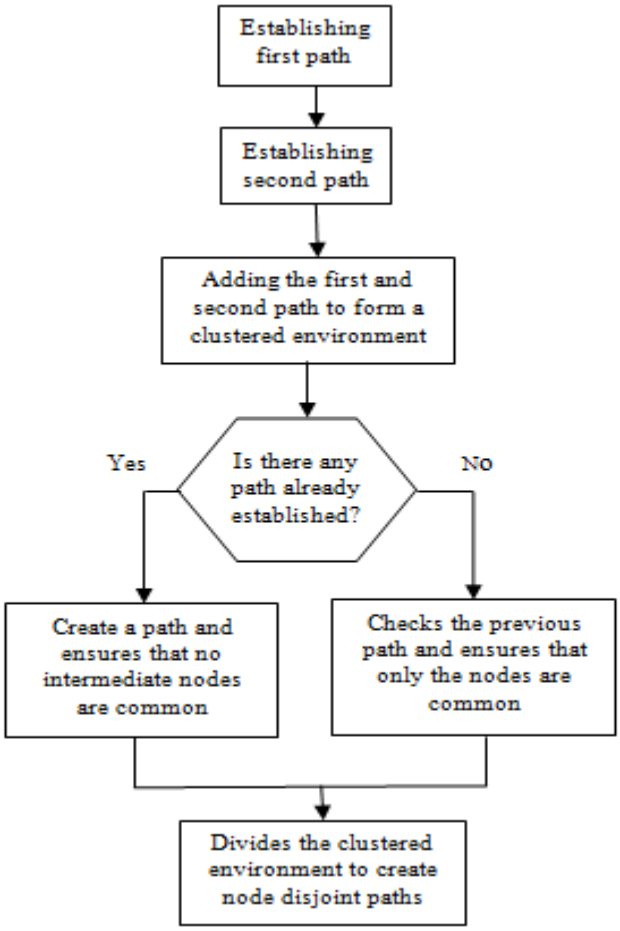

Figure 3.Flowchart for node disjoint multipath routing

In SEAMMRP, wireless sensor network is framed in such a way that it consists of a number of levels for data transmission based on the number of hops between the source and the sink node. Every node can communicate with the sink node. Multiple paths are available between the sources and sink. In level 1, the source nodes communicate with their sink node. In level 2, sink node sends the data to the destination via a common path. This can be chosen based on the hop count and path cost.

Since multiple paths are available, shortest path will be selected with multiple hops. This will prevent the looping between the paths and residual energy consumption will be reduced. The working of this protocol has two main components: (i) Route Establishment and (ii) Data Transmission.

A. Route Establishment:

SEAMMRP protocol is a sink initiated; proactive multi path and multi hop routing protocol. The route establishment is based on the EENDMRP Protocol. The sink node starts with the multiple path route construction to generate its routing tables. The route construction is done with the extension of

two more fields such as Sink ID and path cost as shown in below Fig.4.

Sink ID	Packet type	Hop count	Forward ID	Threshold Energy	Routing path	Path cost	Forwarder's public key

Figure.4 Route Request (RReq) packet frame format

During the routing process, the route request (RReq) packets are communicated between the nodes.Each sensor node multicasts the RReq packet once and maintains its routing table.The RReq packet format consists of the following fields:

a. ***Sink ID-*** to know from which sink the packet is received since multiple sinks are used,
b. ***Packet type-*** to differentiate between the control packet and data packets,
c. ***Hop count-*** number of hops between the source and sink node,
d. ***Forward (source) ID-*** original sender of the network,
e. ***Energy threshold-*** maximum threshold energy level of the sensor node,
f. ***Routing path-*** The way that the packet is traversed from source to sink node
g. ***Path cost-*** based on distance between two nodes and residual energy
h. ***Forwarder's public key-***source nodes public ID known to both sender and receiver

If there is no route to the sink via the node that received route request packet, then that node processes the RReq 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 RReq packet is processed; otherwise the packet is dropped. The node that receives the RReq packet, updates the RReq packet. The updated RReq 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 request packet updates its routing table information such as node's hop count and routing path to the sink node. Similarly, all the nodes in the network receive the route request packet and update their routing table.

After the routing path is identified, path cost is calculated using (2).When the distance between the nodes increases or residual energy is below the threshold value, path cost will increase and that corresponding packet is ignored for further transmission; otherwise the packet is transmitted in the shortest path with multipath and multi hop routing strategies. This process is repeated until all the nodes in the network generate their routing table.

Sink ID	Node ID	Hop count	Node cost	Residual Energy	Node Disjoint Paths	Neighboring node's public key

Figure.5.Format for Routing Information table

The routing table contains node id, number of hops away from the sink, node weight, residual energy, possible disjoint paths between that node to the sink node and neighboring node's public key. The format of the routing table is shown in Fig.5.

B. Optimal Data Forwarding Mechanism:

In the optimal data forwarding mechanism, the primary path should be selected for sending or receiving any data. The primary path is selected based on the multiple disjoint paths from source to the sink based on path cost. To calculate the path cost, the parameters considered here are like the rate of energy consumption, the number of hops it should be transmitted and residual energy before processing starts are taken into consideration. Energy consumption can be divided into three different tasks: sensing, communication and data forwarding. Among the three tasks, data transmission and reception consumes high energy than others. Propagation energy costs are same for both transmission and reception. Energy consumption for a bit needs 0.01mW. On a 5mW processor running at 4 MHz, each instruction requires 0.00002mW. Energy consumption for processing each instruction is less than two orders of magnitude than that for communication. Thus computation energy is not taken into account. For example, assume that the sensing and communication energy costs of each packet is 50mW and 100mW, respectively and also assume that the initial energy on each sensor node is fixed, say 1 kW. So the base station is aware of the energy consumption of each node travelling over the routing path and in intermediate nodes.

The base station will decrease the energy available in the intermediate nodes along the routing path and on the source by 200W (communication) and 150W (sensing) respectively [19]. The rate of energy consumption of node k is calculated to find the path cost of that node. From the energy consumption rate, residual energy drain rate of each node per unit time can be found. The rate of energy consumption increases as the traffic entering a node or intermediate node through which number routing path to sink increases. The packets buffered in node k are also taken into account for calculating path cost. Each and every node in the routing path calculates its path cost taking the above said parameters into consideration.

The ability of handling the data traffic by any node in the path decreases when the path cost of that corresponding node is less. It may be due to lower residual energy or higher energy consumption rate of the node. The cost of the path $Path_i$ is the minimum of the path cost of all the nodes in the routing path $path_i$. This proves that the data handled by the node is based on the path cost of the individual nodes. By this, main path PrP is chosen as the path having maximum cost value compared to all other paths through that node or other node disjoint paths in the network. From these statements, the reliable path is the path that contains node handling the maximum traffic. Let m be the number of multipath between the node k and sink and n_{ik} be the number of nodes in the path $path_i$, ECR_{pre} is the previous energy consumption rate, ECR_{cur} is the current energy consumption rate and ECR_k is the average energy consumption rate of the node k. ECR_k is calculated using the recursive model Exponential Weighted Rolling Mean (EWRM) technique

$$ECR_{cur} = \alpha * ECR_{init} + (1 - \alpha) * ECR_{pre} \text{----} \quad (3)$$

$$ECR_{ik} = \sum (ECR_{cur} + ECR_{pre}) / \sum (n_{i1}, n_{i2}, \ldots n_{ik}) \text{- -(4)}$$

Where coefficient α represents the degree of weighting decrease, a constant smoothing factor between 0 and 1. The value of α is taken as 0.3 based on the present condition of energy consumption by the nodes. Let QL_k be the filled queue length of the node m, RES_k be the residual energy of the node k and NOC_k be the node cost of the node k.Then

$$NOC_k = (RES_k / ECR_k) * QL_k \text{ -----} \quad (5)$$

The path cost of the path $Path_i$ is

$$pathcost_i = \min \{NOC_{k,} \text{ where } k \square n_{ik}\} \text{-------} \quad (6)$$

The main path PrP among the multipath between source and sink is selected as

$$PrP = \max \{pathcost_i \text{ where, } n_{i1} \in m\} \text{ -------} \quad (7)$$

VI. SECURITY IN SEAMMRP

Due to stringent key management in symmetric key algorithms, EENDMRP uses asymmetric (public) key crypto system in which RSA algorithm is used to generate private and public keys. The authenticity of a message is checked by creating a digital signature of the message using the private key, which can then be verified by using the public key but practically only a hash of the message is encrypted for signature verification purposes. Though these security techniques do not provide efficient solution especially for the problems related to integer factorization and discrete logarithm, it is used for easy computation and decrease in encrypted message size [1]. Digital signature based security provides data integrity, confidentiality, privacy, authentication and non-repudiation. MD5 hash function with (Secure Hash Algorithm) SHA-1 is used to generate digital signature in EENDMRP but it causes threat to secure socket layer and collision attacks [1]. SHA-2 is stronger than SHA-1 in that message size can be maximized. Though several security techniques not suited to deploy resource-constrained light weight sensor nodes, RSA based secure hash algorithm (SHA-2) is used to solve this problem. The SHA-2 algorithm is slightly slower than MD5 but the larger message digest generated by it makes more secure against brute-force collision and inversion attacks.

SHA-2 consists of four versions such as SHA-224, SHA-256, SHA-384 and SHA-512 with hash value lengths of 224,256,384,512 bits respectively. Among these variations, SHA-512 is used as security logic for our proposed work. SHA-2 needs only 2^{69} operations to find the collision attack as compared to 2^{80} operations needed in case of SHA-1.This result makes the system to transition towards SHA-2.

A. RSA Public Key Cryptanalysis in SEAMMRP:

SHA-512 takes as input a message with a maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks.

The processing consists of the following steps.[21]

Step 1 Append padding bits

The message is padded so that its length is congruent to 896 modulo 1024

Step 2 Append length

A block of 128 bits is appended to the message

Step 3 Initialize hash buffer

A 512-bit buffer is used to hold intermediate and final results of the hash function. The registers (a,b,c,d,e,f,g,h) are initialized to hold the eight 64-bit integers

Step 4 Process message in 1024-bit (128 word) blocks

The heart of the algorithm is a module that consists of 80 rounds where processing is done using Round function

Each round is defined by the following set of equations:

$$T_1 = h + Ch(e,f,g) + (\sum_0^{512} e) + W_t + K_t$$

$$T_2 = (\sum_0^{512} a) + Maj(a,b,c)$$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

where

t	=step number; 0<=t<=79
Ch(e,f,g)	=(e AND f)⊕(NOT e AND g)
Maj(a,b,c)	=(a AND b)⊕(a AND c)⊕(b AND c)
$(\sum_0^{512} a)$	$=ROTR^{28}(a) \oplus ROTR^{34}(a) \oplus ROTR^{39}(a)$
$(\sum_1^{512} e)$	$=ROTR^{14}(e) \oplus ROTR^{18}(e) \oplus ROTR^{41}(e)$
$ROTR^n(x)$	= circular right shift of the 64-bit argument x by n bits
W_t	=a 64-bit word derived from the current 512 bit input block
K_t	=a 64-bit additive constant
+	=addition modulo 2^{64}

Step 5 Output

After all N 1024-bit blocks have been processed; the output from the N^{th} stage is the 512-bit message digest

The behavior of SHA-512 is summarized as follows.

$$H_0 = IV$$

$$H_i = SUM_{64}(H_{i-1}, abcdefgh_i)$$

$$MD = H_N$$

where

IV	=initial value of the abcdefgh buffer
$abcdefgh_i$	=the output of the last round of processing of the i^{th} message block
N	=the number of blocks in the message (including padding and length fields)
SUM_{64}	=addition modulo 264 performed separately on each word of the pair of inputs
MD	=final message digest value

During the route establishment phase, multiple sink transmits RReq packets to its nearest source nodes. The neighboring source nodes that receive RReq packets append the public key. The nearest source nodes in turn broadcast the RReq packets to its own neighbors. This continues until all the nodes in the network update their routing table with public key. Even from the nodes in level 2, the nodes receive the

RReq packets. Upon updating, node uses only public key of next level and ignores without transmitting to its neighbors. The condition is that every node must know about the public key of neighbor nodes that can be reached in one hop.

In the data forwarding phase, the sink nodes receive the *N* number of data through the node-disjoint main path from the source nodes. At the source node, SHA-512 secure hash algorithm HA which is faster and more secure used to generate message digest *MD*. Digital signature created by source is $Dig\text{-}sign = (MD)^d \bmod n$ obtained by encrypting the message digest *MD* with its private key *d* where $n = p.\ q$, *p* and *q* are distinct random prime numbers. The sink node receives *Dig-sign* with data *N (Dig-sign*, *N)* from its one hop distance nodes throughout the path forwarded by the source.

A neighboring node verifies the digital signature by comparing decrypted value of $Dig\text{-}sign^{\ e} \bmod n$ with message digest *MD* after receiving (*Dig-sign*, *N*) and path in the data packet from the source node. The $Dig\text{-}sign^{\ e} \bmod n$ is decrypted using the sender's public key becomes,

$$Dig\text{-}sign^{\ e} \bmod n = ((MD)^d \bmod n)^e \bmod n$$
$$= (MD)^{ed} \bmod n \qquad \text{-----(5)}$$

Little Fermat's Theorem states that if *p* is prime and *p* does not divide an integer *a* then $a^{p-1} \equiv 1 \bmod p$ and part of the Chinese Remainder Theorem says that, if two numbers MD^{ed} and *MD*, are congruent mod *pq* then it is equivalent in checking congruent mod *p* and mod *q* separately $m^{ed} \equiv m \bmod p$ and $m^{ed} \equiv m \bmod q$

Applying these theorems to equation (5) results,

$$Dig\text{-}sign \bmod n = MD \text{ ---------- (6)}$$

If the digital signatures of *MD* generated by the receiver and the decrypted *MD* are equal, and then the receiver accepts the data as the correct one; otherwise it rejects the data as it is altered by the intruder. By generating the route error packet, it informs the sender about the modification of data. This process is iterated between intermediate nodes in every hop of the node-disjoint path from source to destination for assuring the integrity of data. [1]

The encrypted data includes both RSA and hash algorithms. In the above, steps of SHA-512 are given and it is applied to the original message to find the digest value. Next RSA algorithm using Euler's theorem is applied to the message digest *MD*.

a. Choose positive integers e and d satisfying $ed \equiv 1 \bmod \varphi(n)$. Since e and d are positive, we can write $ed = 1 + h\,\varphi(n)$ for some nonnegative integer h.
b. Assuming that m is relatively prime to n, we have $M \equiv MD^{1+h\varphi(n)} \equiv MD(MD^{\varphi(n)})^h \equiv MD \pmod n$ where the last congruence directly follows from Euler's theorem.
c. When *MD* is not relatively prime to n, the argument just given is invalid. This is highly improbable (only a proportion of $1/p + 1/q - 1/pq$ numbers have this property), but even in this case the desired congruence is still true.
d. It can be either $MD \equiv 0 \bmod p$ or $MD \equiv 0 \bmod q$.

B. Shielding WSN against various attacks:

In addition to the various attacks identified like routing information tampering, Sybil attacks, HELLO flood attacks, selective forwarding, sink and worm holes and Byzantine attacks, the proposed routing protocol also preserves the network from general categories of attacks on hash functions such as brute force and cryptanalytic attacks.

a. Wormhole and Sinkhole attacks:

The traffic is being allured from each sensor node towards the base station by the malicious node of the attacker. Since wormhole uses the dedicated channel of its own it is difficult to detect. Routing protocols involving advertisement messages for topology information is easily affected by sinkhole attack and the probability of verifying it also difficult. In SEAMMRP, source node selects the node-disjoint path, neither by base station nor by sink nodes. According to maximum energy level on each node at different points of time along multi hop node-disjoint multipath, the route selection is changed frequently. So the suspicious node transmitted to compromise the nodes has no effect. If it is injected in-between the source and sink, it lifetime is too short to make the difference.

b. Selective forwarding attack:

Malicious node refuses to forward the incoming message by dropping it either on the routing path and thus prevented from further transmission in case of selective forwarding attack. For effective attack, the attacker injects the suspicious packet on the dataflow path. In SEAMMRP, the node-disjoint routing paths are uniquely chosen by the source node based on the information in the routing table. In addition to this, intermediate nodes have information about its neighbors so the compromising nodes can be detected immediately in the next following hop. Thus message dropping is avoided by preventing the diversion of data traffic by the malicious node.

c. Byzantine Attack:

In Byzantine attack, loop formation on routing path, packet forwarding in unfavorable route and partially dropping the information is done by the suspicious node or a set of malicious nodes. However the network visibly does not show the malfunction action to detect the attack, so it is very hard to identify. In SEAMMRP, routing protocol considered is a sink initiated, proactive multi hop, multipath one. So the routes are discovered by the sink node in the route establishment phase itself.

R Req packets are transmitted only to the next stage nodes not for the previous stage nodes, thus avoiding the formation of loops in the network. From the routing table, node-disjoint multipath is selected between source and destination nodes, so the unfavorable path selection is thus eliminated. Moreover the source selects the main and node disjoint paths in the network.

d. Collision Resistant Attacks:

A brute-force attack does not depend on the specific algorithm but depends only on the bit length of the hash value in the case of a hash function. To ensure the long-term robustness of applications that use hash functions, SHA-1 is

replaced with SHA-2. In spite of complexity, the algorithm is more collision resistant as each input bit can be mapped to more than one hash code.

e. Cryptanalytic attacks:

This type of attack depends on the pitfalls in a particular cryptographic algorithm but not on the bit length of the hash value. In SHA-512, the hash function takes an input message and partitions it into L fixed-sized blocks of b bits each. So the inclusion of the total length of the input to the hash function in the final block makes the job of the opponent more difficult. Either the opponent must find two messages of equal length that hash to the same value or two messages of differing lengths that together with their length values hash to the same value.

VII. PERFORMANCE RESULTS

For experiment, Network Simulator 2.34 is used for implementing SEAMMRP model. The simulation parameters considered are 200 × 200 sq.m area, 10 to 100 numbers of nodes with grid topology, 802.15.4 MAC layer and two ray ground radio propagation models. In SEAMMRP, parameters such as packet delivery ratio, end-to-end delay, packet loss and average energy consumed are compared with AOMDV protocol [7]. The comparison results of the aforesaid parameters of AOMDV and SEAMMRP protocols for varying number of nodes is shown in figures 6,7,8 and 9.The standard parameters set up for network simulator is shown in Table I.

A. Packet-Delivery Ratio(PDR):

PDR is expressed as,

$$\frac{\sum \text{Number of packet received}}{\sum \text{Number of packet transmitted}}$$

In fig.6, comparing PDR with the variation in the number of nodes, delivery rate of packets is increased linearly in SEAMMRP protocol against AOMDV. That is, the number of packets lossed is less in SEAMMRP due to the selection of main path (PrP) from the routing table having maximum as compared to AOMDV. The path selection for sending and receiving any data in the SEAMMRP model is based on the path cost which is identified in the routing table. The minimum value of the node's cost is considered as a cost of that particular path. The packet delivery ratio is indirectly proportional to the number of nodes. As number of nodes gets increased, the PDR decreases depending on the packet drops. When the number of nodes is 40 to 50, the packet delivery ratio in SEAMMRP is 100% to 97.5% respectively; which is 97% to 96% in AOMDV model. In the SEAMMRP model multiple paths are selected from the source node to sink node and data transmission takes place through multiple hops.

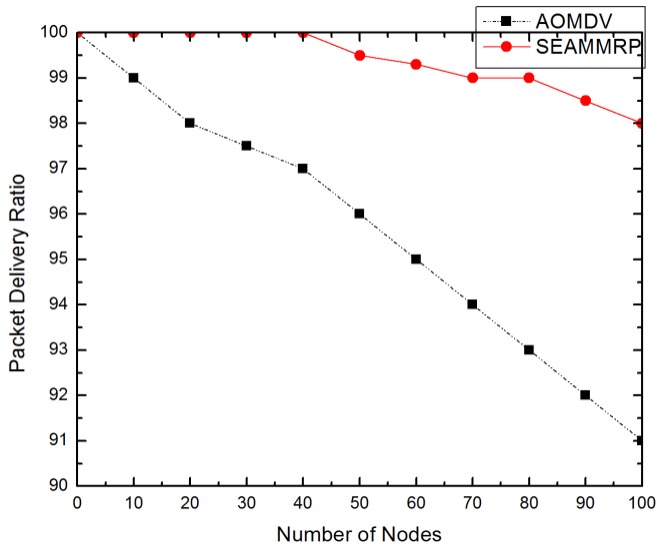

Figure.6 PDR versus Number of Nodes

In the AOMDV model, data transmission is based on the random path selection through multiple paths. When number of nodes increased to 100, the PDR ratio is 98.2% in the SEAMMRP model whereas in AOMDV it is 90.8%. The PDR ratio is on an average of 7.4% higher than the AOMDV model.

B. Average End-to-End Delay:

End-to-end delay includes delay incurred due to propagation, queuing, route discovery, data storage and processing. Due to the presence of multiple sinks in SEAMMRP model, data can be transmitted in multiple paths in such a way that various segments of packets can be reached to sink at the same time, thus reducing the transmission delay. Fig.7 shows the average end-to-end delay when the number of nodes increased from 10 to 100. When nodes are 50, the delay is 25% less as compared to AOMDV model. When nodes are increased, the delay also slightly increased. The end-to-end delay is on an average of 27.11% reduction in SEAMMRP as compared to AOMDV model.

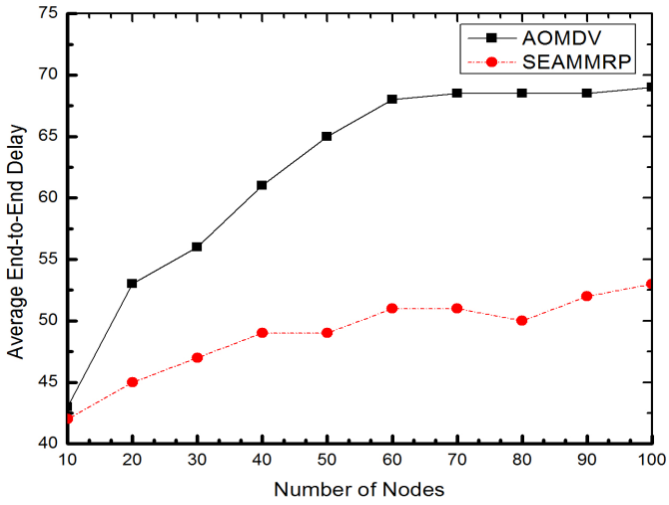

Figure.7 Average End-to-End Delay versus Number of Nodes

C. Packet Loss:

Packet loss is based on the path selection and buffer length. Compared to AOMDV model, packet loss is greatly reduced in SEAMMRP model. When number of nodes increased, there is a possibility of packet loss in queue length of the source or sink node's routing table. When nodes are 30 to 40, loss is 5% in AOMDV and 1% in SEAMMRP model. When nodes increased to 100, the packet loss is 64% in SEAMMRP model, whereas in AOMDV model it is 90%. Since random path selection is used, there is a possibility of data loss in AOMDV and these constraints are removed when path selection is done in reactive nature and transmission is through multiple hops.

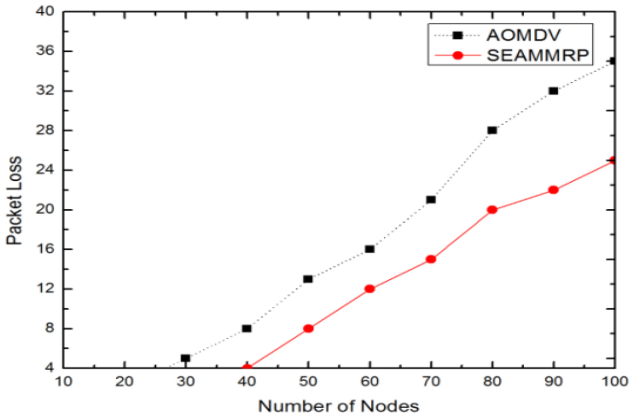

Figure.8 Packet Loss versus Number of Nodes

D. Average Energy consumed:

In the proposed multi hop and multipath routing protocol, average energy spent by the sensor nodes in the network is a prominent thing for the energy efficiency. The average energy consumed by each node in the network is shown in fig.9. Compared to the AOMDV model, the average energy consumed by each sensor node is greatly reduced in SEAMMRP model. In the SEAMMRP model, since the route construction is reactive in nature, routing tables are constructed by all the nodes in the network and path is found before transmission. Only on-demand route construction is possible in the AOMDV model. Thus for the establishment of route, requirement of energy is greatly reduced. In SEAMMRP model, energy consumed is 20% less than the AOMDV model.

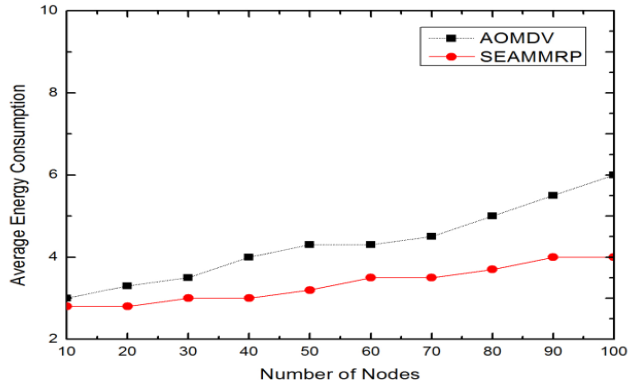

Figure.9 Average Energy Consumption versus Number of Nodes

Table 1: Simulation of Model Parameters

S.No	Parameters	Values
1.	Simulation area	200x200 m^2
2.	Propagation	Two ray ground
3.	MAC type	802.15.4
4.	Queue type	DropTail
5.	Queue limit	100
6.	Antenna type	Omni directional antenna
7.	Transmission range	15 m
8.	Number of nodes	10 to 100 nodes
9.	Packet type and size	CBR and 512 bits
10.	Data rate	100 KBPS
11.	Simulation Time	150s
12.	Topology	Grid
13.	Initial energy	5 J
14.	Transmission Power	100mW

VIII. CONCLUSION WITH FUTURE EXTENSION

Wireless Sensor Networks (WSN) finds increasingly new research areas as the information technology advances. Advance in technology introduces new application areas for Wireless Sensor Networks (WSN). Due to the application of Wireless Sensor Networks in the critical operations involved in the fields of military, medical, space communication etc., extending the endurance of the network and protecting against threats is an important apprehension. In our proposed work, an energy-aware multi hop, multipath secure routing is developed for Wireless Sensor Networks that ensures integrity of data. In SEAMMRP, both enhanced energy-aware and security techniques are implemented that results better packet delivery ratio, end-to-end delay, energy conservation and thus providing Quality of Service with link reliability. Security is improved by using SHA-2 hash function with RSA and creating digital signature for this hashing mitigates various attacks such as wormhole attack, sinkhole attack, selective forwarding attack, byzantine attack, collision resistance attack and cryptanalytic attacks. NS-2 Simulation experiment shows improvement in the above said parameters while comparing with AOMDV routing protocol. In packet delivery ratio, there is an enhancement of 7.4% thus reducing the packet loss, 27.11% decrease in an average end-to-end delay and energy consumption is reduced up to 20% as compared to AOMDV model.

In SEAMMRP, the routing protocol consideration is limited to text based information flow and does not focus on multimedia data transfer. The research issue can be extended with this concept.

IX. REFERENCES

[1] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad," Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE SENSORS JOURNAL, VOL. 12, NO. 10, 2012, pp.2941-2949.

[2] 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.

[3] Mohammad Hammoudeh_, Alexander Kurz†, andElena aura,"MuMHR:Multihop,Multipath Hierarchical Routing", International Conference on Sensor Technologies and Applications,SensorCommSENSORCOMM,2007DOI:10.1109/SENSORCOMM.2007.4394911.

[4] Marjan Radi, Behnam Dezfouli, Kamalrulnizam Abu Bakar and Malrey Lee, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", Sensors 2012, 12, 650-685; doi: 10.3390/s120100650.

[5] A. V. Sutagundar*, S. S. Manvi**, Kirankumar. B. Balavalad," Energy Efficient Multipath Routing Protocol for WMSN's", International Journal of Computer and Electrical Engineering, Vol. 2, No. 3, June, 2010.pp. 503 -510.

[6] Y. K. Tan, Sustainable Wireless Sensor Networks. Rijeka, Croatia: Intech Publishers, Dec. 2010, ch. 12, pp. 279–309.

[7] Mahesh K. Marina1*, † and Samir R. Das2, "Ad hoc on-demand multipath distance vector routing", Wireless Communications And Mobile Computing,Wirel. Commun. Mob. Comput. 2006; pp.969–988.

[8] Jie Zhang, Choong Kyo Jeong, Goo Yeon Lee, Hwa Jong Kim," Cluster-based Multi- path Routing Algorithm for Multi-hop Wireless Network", International Journal of Future Generation Communication and Networking, Vol.1,2008.

[9] Ram Kumar E,Vinothraj N,Kiruthiga G," Energy Based Multipath Routing Protocols for Wireless Sensor Networks", Journal of Computer Applications,Volume-5, 2012,pp.190-197.

[10] R Vidhyapriya, Dr.P.T.Vanathi," Energy Efficient Adaptive Multipath Routing for Wireless Sensor Networks", IAENG International Journal of Computer Science, 34:1, IJCS_34_1_8.

[11] Ye Ming Lu and Vincent W.S. Wong," An Energy-Efficient Multipath Routing Protocol for Wireless Sensor Networks", Natural Sciences and Engineering Research Council of Canada under grant number 261604-03.

[12] Samina Ehsan and Bechir Hamdaoui," A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks", IEEE Communications Surveys & Tutorials, vol. 14, no. 2, second quarter 2012.

[13] Ahmed E.A.A. Abdulla, Hiroki Nishiyama,Jie Yang, Nirwan Ansari and Nei Kato,"HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs", IEEE Transactions On Wireless Communications, Vol. 11, No. 7, July 2012,pp. 2531-2541.

[14] 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.

[15] C.-S. Nam, H.-Y. Cho, and D.-R. Shin, "Efficient path setup and recovery in wireless sensor networks by using the routing table," in Proc. Int.Conf. Educ. Technol. Comput., 2007, pp. 156–159.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] William Stallings," Cryptography and Network Security Principles and practice", published by Dorling Kindersley (India) Pvt. Ltd., licensees of Pearson Education in South Asia,5th Edition,2011.

[22] http://en.wikipedia.org/wiki/RSA_algorithm

