Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks

Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad

***Abstract*— The objective of energy efficient routing protocol is to increase the operational lifetime of the wireless sensor networks. Multipath routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple paths instead of a single optimal path. Transmission of secured data is also an important research concern in the wireless sensor networks. In this paper, a 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. It is compared with an ad hoc on-demand multipath distance vector routing protocol. It shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multipath distance vector routing.**

***Index Terms*— Digital signature crypto system, multipath routing protocol, node-disjoint, security, wireless sensor network.**

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 [1]. 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) 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. The security threats to the WSN like spoofing or altering the route information, selective forwarding, sinkhole attack, sybil attack and byzantine attack are addressed. It provides more security by using the digital signature crypto system. This crypto system uses the MD5 hash function and RSA algorithm. The rest of this paper is organized in the following manner. In section 2, the existing work is discussed. The network assumptions are mentioned in section 3. In section 4, public key cryptography in wireless sensor networks is discussed. The energy efficient node disjoint multipath routing is presented in section 5. In section 6, security in the EENDMRP is discussed. In section 7, the simulation results and discussion are provided. Conclusions are presented in section 8.

II. Related Works

Marina et al [11] 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

Manuscript received March 1, 2012; revised May 17, 2012; accepted May 31, 2012. Date of publication June 22, 2012; date of current version August 7, 2012. The associate editor coordinating the review of this paper and approving it for publication was Prof. Paul C.-P. Chao.

S. M. G. and R. J. D'Souza are with the Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Mangalore 575025, India (e-mail: kgshivam@gmail.com; rjd@nitk.ac.in).

G. Varaprasad is with the Department of Computer Science and Engineering, BMS College of Engineering, Bangalore 560004, India (e-mail: drvaraprasad@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSEN.2012.2205674

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.

Choon-Sung Nam et al [13] proposed an efficient path set up and recovery in WSNs. This mechanism is a sink initiated, query based routing protocol. It is a variant of directed diffusion routing protocol. This mechanism finds the optimal path between the source and destination based on the minimum number of hops. But setting up of the multiple paths is not shown.

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.

Power-Aware Node-Disjoint Multi-Path Source Routing (PNDMSR) [15] is a reactive protocol and source initiated routing protocol. The route discovery in the PNDMSR model is similar to route discovery in Dynamic Source Routing (DSR) [16]. In the PNDMSR model, only the destination node is allowed to send the RREP packet to the source node, while in the DSR model, the RREP packets is sent by the intermediate and destination nodes. The node-cost field is added in the RREQ packet and carries the cumulative cost. In PNDMSR, the RREQ is generated by the source node. The RREQ packet is broadcasted in the network. The destination node, after receiving RREQs sends the RREP in the reverse path. If the network is dense, identifying the multiple node disjoint paths is cost effective. The number of control messages used may be higher.

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. Assumptions

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 $E \subset VXV$. The link $(i, j) \in E$, 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.

IV. Public Key Cryptography in Wireless Sensor Networks

Public key encryption is a cryptographic method which uses asymmetric-key pair: a public key and a private key. Asymmetric key pair is used to encrypt and decrypt messages. The public key is made public and is distributed widely and freely. The private-key need not be distributed and it is kept secret. In public key cryptography, data encrypted with the public key can only be decrypted with its private key; conversely, data encrypted with the private key can only be decrypted with its public key. This characteristic is used to implement encryption and digital signature. The digital signature in public key encryption provides the authentication security in the system. The highlight of public key cryptography is in providing confidentiality without sharing the private keys. In general, public key cryptography is best suited for an open multi-user environment [19].

Public key crypto system's counterpart is the symmetric key crypto system and is also used in WSN security. The symmetric key crypto system, uses the same key for both encrypting and decrypting data. Many researchers proposed different symmetric key distribution (sharing) techniques for WSNs [20]–[23]. These algorithms are relatively easy to implement. It needs only limited computation power for encryption which (at least some of them) are known to be hard to break even with massive resources. Symmetric key system expects that, all participating nodes have to agree on a common key prior to exchanging data. One simple solution is to replace the common key very frequently at small time intervals for securing WSNs. This periodically shared new key may induct control overhead in the network if, periodicity is very small and WSNs size is large. This solution is the simplest way for securing WSN. It uses a single shared key to encrypt traffic over the network, and this key may be periodically updated to ensure more security against eavesdropping [24].

In the recent past various researchers attempted to implement security in WSNs using public key encryption. Public key cryptography provides authentication and confidentiality. The high processing overhead and energy cost make the implementation of public key cryptography in WSNs impractical. Few researchers proposed mechanisms to reduce processing and energy cost in Elliptic curve cryptography (ECC) [25].

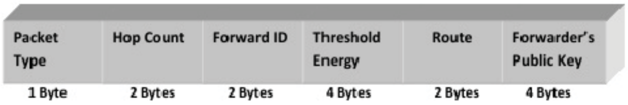
V. Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP)

In EENDMRP, WSN is assumed to consist of a number of stages St_i, i $= 1, 2, \ldots, l$ based on the number of hops between the source and destination. The sink is a stage zero, St_0 node. Every node can communicate with sink node in stage St_1. We assume that a stage St_i node can communicate with nodes on the same stage St_i and next stage St_{i+1}. But, it cannot communicate with stage St_{i-1} nodes. This prevents the formation of paths with loops. Initially all the nodes in the network except the sink node have very high hop count value. Initially, all the nodes have its residual energy level above the threshold energy value. We discuss the working of EENDMRP in detail in two phases: (i) route construction phase and (ii) data transmission phase.

A. Route Construction Phase in EENDMRP

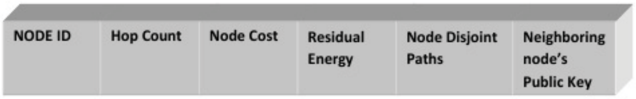
EENDMRP is a sink initiated, proactive node disjoint multipath routing protocol. The sink node starts the multipath route construction phase to generate its routing tables. During this process, Route CONstruction (RCON) packets are exchanged between the nodes. Each sensor node broadcasts the RCON packet once and maintains its own routing table. The format of the RCON packet is as shown in the Fig. 1. It has packet type (to differentiate between control packet and data packets), beacon hop count (Number of hops away from the sink), beacon source (original sender of beacon), node threshold energy level, Path (packet traversed from sink to node) field and forwarder node's public key. 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. 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. 2.

The route-construction phase is illustrated with the following example. The network in Fig. 3 is a 10 node network. The node D is the sink. The sink node initiates the route construction phase by broadcasting RCON packet to its neighboring nodes i.e., nodes 4, 6 and 9. The node 4 receives the RCON packet from the sink node. It updates its routing table if its residual energy is above the threshold energy value and its hop count is greater than the RCON packet hop count. Node 4 rebroadcasts the RCON packet to its neighboring nodes 3, 6 and sink node. The node 6 and sink node discard the RCON packet sent from the node 4, since its hop count value is less than the RCON packet hop count. The node 3 receives the RCON packet from the node 4 since its hop count value is



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.



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

Fig. 2. Format of node routing table.

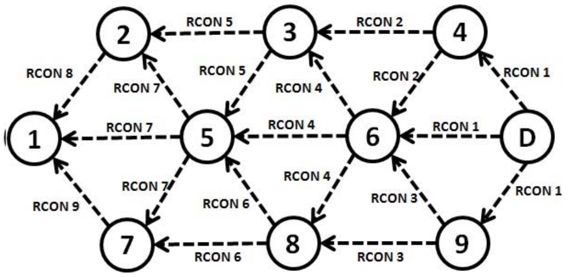


Fig. 3. Route construction phase in EENDMRP.

greater than the received RCON packet hop count. The node 6 updates the RCON packet received by the sink node and broadcasts to its neighboring nodes. Here, the nodes 3, 5 and 8 receive the packet. But, the nodes 4, 9 and sink node discard the packet as their hop count is less than the received RCON packet hop count. Similarly, node 9 updates the RCON packet received by the sink node and broadcasts to its neighboring nodes. Here, the nodes 6, 8 and sink receive the RCON packet. The node 6 and sink discard the RCON packet sent from the node 4, since its hop count value is less than RCON packet's hop count. This will be continued until all the nodes in the network generate their routing tables.

B. Data Transmission Phase in EENDMRP

In this phase, the primary path is chosen from the available node disjoint multiple paths between source and destination based on maximum Path Cost (PC). To choose primary path based on maximum path cost, the effective node parameters like, rate of energy consumption, filled queue length and effective residual energy is taken into consideration. To identify the path cost, the rate of energy consumption of j^{th} node is calculated. It is better to identify the rate of energy consumption to have knowledge of the rate of drain of the residual energy of a node for a unit time. If the data traffic through the node is high, or if that node acts as an intermediate node for large number of routes to sink, then the rate of energy consumption is also high.

To calculate j^{th} node cost, the data packets queued up in the j^{th} node's buffer is also taken into consideration. Every node in the path finds its cost. If node cost is low, then the capability of handling the data traffic by that node is less, as it may have higher rate of energy consumption, or lower residual energy. If the j^{th} node has the minimum node cost compared to all the nodes in the path Pi, then j^{th} node cost becomes the cost of the path Pi. This is to confirm that, the data traffic through the path is to suit the capability of the least cost node.

Similarly, if all the path costs $PC_i i = 1, 2, \ldots, k$ 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 P_i, RECold 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

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

where, the coefficient $\alpha \in (0, 1)$ 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

$$NC_j = (RE_j / REC_j) * FQL_j. \tag{2}$$

The path cost PC_i of the path P_i is

$$PCi = \min\{NC_j \quad \text{where,} \quad j \in m\}. \tag{3}$$

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

$$PP = \max\{PC_i \quad \text{where,} \quad i \in k\}. \tag{4}$$

VI. Security in EENDMRP

The security in EENDMRP is designed 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 is 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 is used to create message digest $H(M)$ at the source node. The source node generates the digital signature $d_{sign} = (\text{H (M)})^d$ 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 $p \neq q$. 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 d^e_{sign} 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

$$\begin{aligned} d^e_{sign} mod\ n &= ((H(M))^d mod\ n)^e mod\ n \\ &= (H(M))^{ea} mod\ n \end{aligned} \tag{5}$$

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

$$d^e_{sign} mod\ n = H(M) \tag{6}$$

If the generated $H(M)$ by the receiver and the decrypted $H(M)$ of digital signature dsign 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.

A. 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 $d_{sign} = ((H(M))d$ mod $n)$ and decrypted using source public key e

$$\begin{aligned} H(M) &= (d^e(mod\ n)) \qquad (7) \\ &= ((H(M)^d)^e(mod\ n)) \\ &= (H(M))^{ed} mod\ n \\ &= (H(M))^{1+k(p-1)(q-1)} mod\ n \\ H(M) &= (H(M)).(H(M))^{k(p-1)(q-1)} mod\ n \end{aligned}$$

using, $ed \equiv 1$ mod $(\varphi(n))$ and replacing $(\varphi(n))$ 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 $a^{p-1} \equiv 1$ mod p. Hence

$$H(M)^{p-1} mod\ p = 1. \tag{8}$$

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

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

on rearranging (9) is equivalent to

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

using (8) it is equivalent to $H(M)$. Similarly

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

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

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

from Equation (7)

$$H(M) \equiv H(M)(mod\ n) \text{ since, } n = p.q.$$

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

B. Defending the WSN Threats

The specific wireless sensor network attacks defended in this work are: data tampered or altered routing, Sybil attack, HELLO attack, selective forwarding, sink hole and byzantine attack.

1) Defending Data Tampered or Altered Routing
The most direct attack against routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false-error messages, partition the network, increase end-to-end delay etc. In digital signature based crypto system, public key of the sender is required to decrypt the message digest at the data receiver node. If the decrypted digital signature and the evaluated

message digest at the receiver is equal, then it proves the data integrity and non-repudiation in the network.

2) Selective Forwarding and Sink Hole
Multi-hop networks are often based on the assumption that participating nodes will faithfully forward received messages. In selective forwarding attack, the malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet that it receives. In the EENDMRP model, there is no chance of the malicious node to drop the packets or to divert the data traffic in the network, because the source node selects the node-disjoint path to route the data from its routing table. Every intermediate node knows its next neighbouring node. So there is no chance of malicious node diverting the data traffic.

3) Byzantine Attack
In this attack, a compromised node or a set of compromised nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets in non-optimal routes and selectively dropping packets. It is very difficult to detect the Byzantine attacks, since the networks do not exhibit any abnormal behavior. The EENDMRP model is a sink initiated, proactive multipath routing protocol. The routes are constructed in the route construction phase, which is initiated by the sink node. Every node in the network can communicate or forward the RCON packets to its next stage nodes and not with the previous stage nodes. This mechanism avoids the formation of loops. The node disjoint multi path from the source to sink node is selected from its routing table. Selecting a non-optimal path by the malicious node to the sink node is not possible. The primary path and node disjoint paths are selected by the source node.

TABLE I
SIMULATION PARAMETERS

Sl.No	Parameters	Values
1	Simulation area	200 × 200 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	150 s
12	Topology	Grid
13	Initial energy	5 J
14	Transmission power	36.00e-3 W
15	Reception power	20.00e-3 W
16	Idle power	20.00e-3 W
17	Sleep power	1.00e-6 W

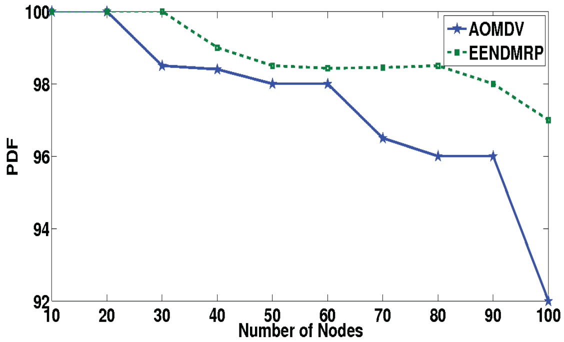


Fig. 4. Variation of PDF with number of nodes.

VII. RESULTS AND DISCUSSION

The EENDMRP model is implemented using Network Simulator 2.34. The simulation parameters 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. The EENDMRP model is compared with the AOMDV model [3] from different perspectives such as packet delivery fraction, end-to-end delay, normalised routing load and average energy spent. The network simulator set up is shown in Table I.

A. Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF). Fig. 4 shows the PDF of the AOMDV and EENDMRP models for varying number of nodes. The PDF is always high in the EENDMRP model as compared to the AOMDV model. The number of dropped packets in the EENDMRP model is less than that in the AOMDV model. The effective primary path selection mechanism in the EENDMRP model avoids the packet drop over the network. The primary path is chosen from the node routing table based on the maximum path cost in the EENDMRP model. The path cost is chosen using filled queue length of the node. The minimum value of the node's cost in the path is the cost of that path. If any node's filled queue length is maximum in a path, then the chances of selecting that path as a primary path is minimized. It indicates that the primary path is selected, such that the residual energy is high and filled queue length is short. The packet drops are avoided in EENDMRP after the queue is filled. In the AOMDV model, the multiple paths are selected from the source node to sink node. In the AOMDV model, random path is selected for sending the data packets from the source node to sink node over the multiple paths. The randomness in path selection makes the path more vulnerable to packet drops in the network. In Fig. 4, when the number of nodes in the network is 40 and 50, the PDF of the AOMDV model is 98% and when the number of nodes is 60, the PDF is 96.5%. In the EENDMRP model, the PDF is an average of 7% higher as compared to the AOMDV model because of queue buffer overflow. When the number of nodes is increased from 10 to 100, the PDF is also

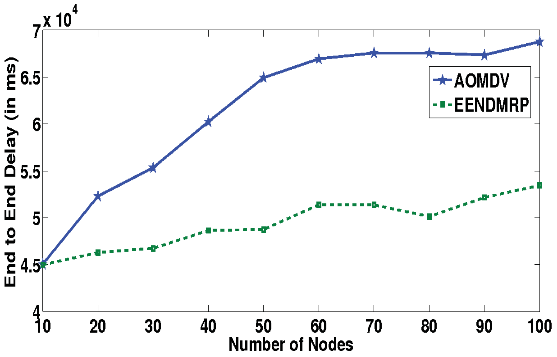


Fig. 5. Variation of end-to-end delay with number of nodes.

decreases. When the number of nodes is 10 and 100, the PDF in EENDMRP is 100% and 97% respectively; which is 100% and 92% in AOMDV.

B. Average End-to-End Delay

Average end-to-end delay includes all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets. Fig. 5 shows the end-to-end delay incurred in sending the data from the source node to sink node in the AOMDV and EENDMRP models. The end-to-end delay is reduced in the EENDMRP model as compared to the AOMDV model. The EENDMRP model is a proactive multi-path 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 RCON 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. The path selected to route the data may not be of the minimum hop. There is a reduction of 28.6% in end-to-end delay in the EENDMRP model as compared to the AOMDV model. When the number of nodes is increased the end-to-end delay also increased, because the number of hops between source and destination also increase. There is 4.5e4 ms and 6.8e4 ms end-to-end delay in AOMDV when the number of nodes is 10 and 100 respectively. But, end-to-end delay in EENDMRP is 4.4e4 ms and 5.3e4 ms when the number of nodes is 10 and 100 respectively. There is an average reduction of 24.71% delay in EENDMRP as compared to AOMDV.

C. Normalized Routing Load

Normalized Routing Load (NRL) is the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. Fig. 6 shows the NRL in the AOMDV and EENDMRP models. In the AOMDV model, the number of control messages used in constructing multiple paths is high as compared to the EENDMRP model. The source node broadcasts the RREQ packets to its neighbours. The RREQ packet is re-broadcast until the destination or an intermediate node receives the RREQ packet. The destination generates multiple route replies. These replies travel along multiple loop-free reverse paths to the source established during the route request propagation. In every node's route construction phase, the number of RREQ packets and its multiple route replies travelled in multiple routes in multi hops consume high routing packet overhead per data packet transmission. As the number of nodes increases in the network or when the number of hops between the source and destination is large, then the control messages is also high. In Fig. 6, when the number of nodes is increased from 50 to 60, the NRL is increased sharply as compared to other cases. This is because, the source selected in the simulation is maximum hop distance node in the network to the destination compared to other cases. The NRL in the EENDMRP model is low compared to the AOMDV model, because of its proactive routing nature. The number of control messages used in the EENDMRP is low. In the EENDMRP model, the RREP packets are avoided from the destination node. The multiple routes are constructed in all the nodes in an iteration of route construction phase. There is a reduction of 67.56% of normalized routing load in the EENDMRP model as compared to the AOMDV model in the network.

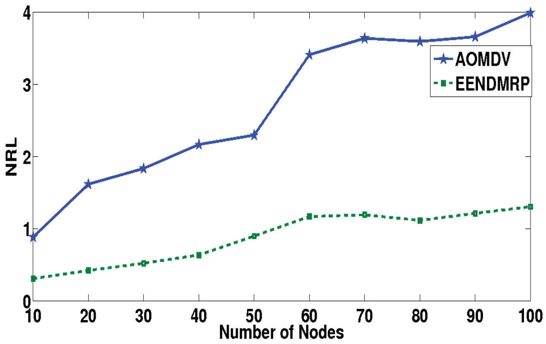


Fig. 6. Variation of NRL with number of nodes.

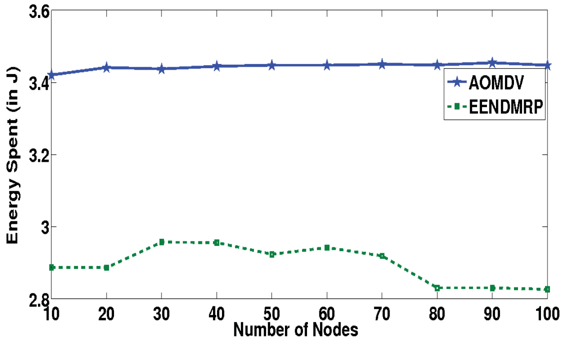


Fig. 7. Variation of energy spent (in Joules) with number of nodes.

D. Average Energy Spent

Average energy spent by the sensor nodes in the network is one of the important metrics to evaluate energy efficiency of the proposed routing protocol. Fig. 7 shows the average energy spent by each node in the network. 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. Thus the energy spent on the route discovery is reduced drastically. There is a reduction of 19.1% in energy consumption in the EENDMRP model as compared to the AOMDV model.

VIII. Conclusion

The work proposes the energy efficient node-disjoint multipath routing protocol to increase the network lifetime. 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. EENDMRP performs better than AOMDV protocol. There is an improvement of 7% in packet delivery fraction, reduction of 28.6% in end-to-end delay, reduction of 67.56% of normalized routing load and energy saving of 19.1%. 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. In this paper EENDMRP is limited to physical data routing and multimedia data routing is not taken into consideration. A new metric measuring energy and QoS with link reliability is yet to be designed.

References

[1] 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.

[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-efcient 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] 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.

[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] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

[21] 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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Sensor networks with public key technology," in *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw.*, 2004, pp. 59–64.

[28] 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.

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

Shiva Murthy G received the B.E. and M.E. degrees in computer science and engineering from Bangalore University, Bangalore, India. He is currently pursuing the Ph.D. degree with the Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal, India.

His current research interests include wireless ad hoc and sensor networks, network optimization, reliability engineering, and cognitive networks.

Robert John D'Souza received the Ph.D. degree from the Indian Institute of Technology, Delhi, India.

He is a Professor with the Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal, India. Currently, he is guiding three Ph.D. students. He has published many journal publications and conference publications. His current research interests include data mining and wireless sensor networks.

Golla Varaprasad received the B.Tech. degree from Sri Venkateswara University, Tirupati, India, in 1999, the M.Tech. degree from Visvesvaraya Technological University, Belguam, India, in 2001, and the Ph.D. degree from Anna University, Chennai, India, all in computer science and engineering.

He is currently an Associate Professor with the Department of Computer Science and Engineering, BMS College of Engineering, Bangalore, India. He has authored or co-authored 35 journal publications and 35 conference publications, and holds four patents and copyrights. He is the author of two textbooks. His current research interests include mobile ad hoc networks.