

DIGITAL SIGNATURE - BASED SECURE NODE DISJOINT MULTIPATH ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

Dr. A.SenthilKumar,
Assistant Professor,
Department of Computer Science,
Arignar Anna Government Arts College,
Namakkal, Tamilnadu, India.

R.Gopalakrishnan,
Ph.D., Research scholar,
Periyar university,
Salem, Tamilnadu, India.

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 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.

Keywords: *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 over flow, routing table poisoning, etc.

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 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 neighboring 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. A source, upon receiving the RERR initiates a new 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 disjointness 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 enactment 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 neighboring 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 are sent by the intermediate and destination nodes. The node-cost field is added in 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 DETeciton (NBR DET) packet to construct the neighbor list in each node. Every node sends the neighbor list information to the base station. The base station generates the pair-wise key for every link in the network. These packets,

neighbor 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 neighbor Discovery (ND) packet, Neighbor Collection (NC) packet and Neighbor Collection Reply (NCR) packet in the routing protocol. The ND packet is broadcast in the network to know the neighboring nodes, the base station node broadcasts NC packet in order to collect the neighbor's information of each node gathered during the previous broadcasting. The sensor nodes acknowledge to the NC packet by sending the neighbor collection reply packet to the base station. The SEEM model justifies the security without using the crypto system mechanism in the routing protocol.

VII. RESULTS AND DISCUSSION

The EENDMRP model is implemented using Network simulation 2.34. The simulation parameters are 200 x 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, normalized routing load and average energy spent.

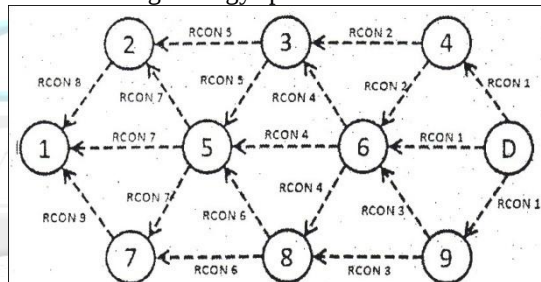
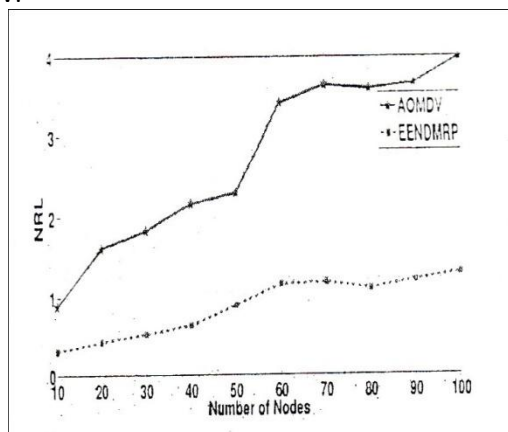


Fig. 3. Route construction phase in EENDMRP.

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 length of the node. The minimum value of the node's path is the cost of that path. If any node's filled length is maximum in a path, then the chances of that path as a primary path is minimized. It incites the residual entering high and filled queue length is short. The packet drop avoided in EENDMRP after the queue is filled. In the AD model, the multiple paths are

selected from the source and to sink node. In the AOMDV model, random path is selection for sending the data packets from the source node to and node over the multiple paths. The randomness in path selection makes the path more vulnerable to packet drops in the In Fig. 4, when the number of nodes in the network is 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 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.



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. 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.

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 selection the primary path in the energy efficient node-disjoint multipath routing protocol. EENDMRP performs better than AOMDV protocol. There is an improvement of 75 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, non-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.AI-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," *JEEE Trans. Parallel Distrib. Syst.*, vol.21, no.6, 00.881-896, Jun.2010.
- [4]. M.-C.Zheng, D.-F.Xhang, and J.Luo, "Minimum hop routing wireless sensor networks based on ensuring of data link reliability," in *Proc. Int. Conf. Mobile Ad-Hoc S 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.