Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130208

Secured Wireless Sensor Network Framework to Support Guaranteed Successful Data Transmission

R. J. Kavitha[1,*] *and N. Satheesh*[2]

[1] Department of ECE, University College of Engineering, Panruti, India
[2] Department of CSE, Chalapathi Institute of Engineering & Technology, Gundur, India

Received: 2 Nov. 2018, Revised: 12 Dec. 2018, Accepted: 28 Dec. 2018
Published online: 1 Mar. 2019

Abstract: We introduce the protocols to perform the optimal and secured routing in the wireless sensor network to guarantee the successful data transmission. In the proposed research method, the previous drawbacks have been resolved by introducing the Secured Edge Disjoint Routing Protocol (SEDRP). Optimal Edge disjoint routing is done by introducing the various research techniques that can ensure the optimal forwarding of the data packets. Optimal selection of edge disjoint route paths is done by using hybrid genetic PSO algorithm. This research work considers the following Quality of Service (QoS) parameters for the optimal selection of route paths: "energy, bandwidth, processing capacity, reliability". The secured data communication is guaranteed by introducing signature-based authentication procedure which would establish the secured communication medium between sender and receiver. The overall simulation evaluation is carried out in NS2 simulation environment from which it is proved that the proposed research method can enhance the routing performances.

Keywords: Secured data transmission, cluster head selection, optimal clustering, cluster head, security.

1 Introduction

Wireless sensor network is an emerging field where lots of research work have been done involving hardware and system design, networking, security factor and distributed algorithm [1]. Sensor nodes normally sense the data packet and transfer it to the base station via some intermediate nodes. The sensor nodes are of low cost, low power and short transmission range [2]. Nodes are used to send the data packet locally to its single hop neighbor nodes, and so on; and finally it reaches to its base station. Initially, nodes are deployed flying from aircrafts randomly and some time node changes its initial position (the time of deployment) and moves across the region based on the requirement; so this type of nodes is called mobile nodes [3]. There are two types of data transmission in wireless sensor network, these are direct transmission and multi-hop data transmission [4].

In direct transmission, data are sent directly to the sink [5] where as multi-hop transmission data is sent via number of intermediate nodes lying between source node and base station [6]. In sensor network, the drift of statistics is very crucial thing because every information packet consists of the occasion which can be very crucial for some software. So records transmission should be secured. However sensor node has limited power and restrained reminiscence capability, so keeping security is difficult for them [7]. It has to be made sure that, the reports from the sensors in motion are authentic and reach the base station without any fabrication or change.

The undertaking of securing Wi-Fi sensor networks is complex because sensors are exceptionally nameless devices with a confined strength and reminiscence capacity; they don't have any information of their locations within the deployment surroundings [8]. To make the data transmission comfy some basic aspects of protection has to be maintained for the duration of transmission. Here, authentication and confidentiality is maintained for the duration of facts transmission because without these two parameters data transmission cannot be dependable [9]; also it mentioned how the missing packets may be detected throughout transmission with the aid of a few efficient strategies.

In the proposed research method, these issues are resolved by introducing the Secured Edge Disjoint Routing Protocol (SEDRP). In the proposed research

* Corresponding author e-mail: rjkavitha@yahoo.com

method, Optimal edge disjoint routing is done by introducing the various research techniques that can ensure the optimal forwarding of the data packets. Optimal selection of edge disjoint route paths is done by using Hybrid Genetic PSO algorithm.

In this section detailed introduction about the wireless sensor network and the security issues are discussed. In Section 2, discussion about the various related research methodologies, which are used to ensure the guaranteed data transmission is given. In Section 3, a discussion about the working procedure of proposed protocol and its benefits along with suitable examples and explanation have been given. In Section 4, a discussion about the experimental results is provided in terms of performance metrics. In Section 5, an overall conclusion of the research work is given based on the resulted simulation outcome.

2 Related Works

The Hierarchical Control Clustering (HCC) [10] is a kind of clustering algorithm which uses breadth first search algorithm for selecting CH and initial CH selection is pre-assigned. When CH goes below the threshold energy, HCC call BFS algorithm to construct spanning tree among sensor nodes and try to select the CH, and note that the CH count is a variable and not a fixed one. The WSN environment applicable here is that field sensors and selected CH sensor do move and so the Hop distance is multi-hop since there is no direct link between CH to all remaining sensor nodes belonging to any cluster.

Another interesting clustering technique for WSN is Less Energy Adaptive Clustering Hierarchy (LEACH) [11] using the randomness for selecting CH and number of CH used for each cluster is variable. The other parameter such as CH mobility is stable here and the major advantage is that once this algorithm selects the CH, then every other node within this cluster has the distance of 1 Hop and this lead reliability for communication. Stable CH (less mobility) and 1 Hop distance are the best suiting parameters for spatiotemporal data transmission between every node-encrypted data to repository node through CH. The Less Energy Adaptive Clustering Hierarchy (LEACH) clustering algorithm is mostly used as application specific, autonomous WSN, equal portability, and long-range communication.

The Energy Optimized Multipath Routing Protocol (EOMRP) [12] algorithm is used mostly in inter-cluster communication application which leads to more relay between Clusters. In this algorithm CH Count is variable, CH selection-based on the proportional ratio between sensor nodes, CH mobility is present and Hop distance is multi Hop. The major drawback in EOMRP is that every node including CH must possess global knowledge about the distance to every other node and sensor's location since this technique following inter-cluster communication.

The Power Efficient and Adaptive Clustering Hierarchy (PEACH) [13] algorithm is comparatively best than LEACH but not suitable for application-specific. The parameters values are as follows. The CH count is gain variable as like HCC, LEACH, and EEUC. The CH selection is based on probability, CH mobility is present and Hop distance is multi Hop just like HCC and EEUC followed.

Kavitha et al. [14] proposed a brand new protocol through integrating power and privateness management techniques called proximal link scheduling and summing homomorphic encryption. In proximal link scheduling, each aggregator nodes in every clusters are allotted to a successive time slot. When the time is allotted, the aggregator node remains in sleep state.

3 Secured Data Transmission in Wireless Sensor Network

In the proposed research method, optimal edge disjoint routing is done by introducing the various research techniques that can ensure the optimal forwarding of the data packets. Optimal selection of edge disjoint route paths is done by using Hybrid Genetic PSO algorithm. This research work considers the following Quality of Service (QoS) parameters for the optimal selection of route paths: "Energy, Bandwidth, Processing capacity, Reliability". In this work, Clustering is done in order to ensure the optimal and reliable data transmission which is done by using density aware optimal clustering approach. This method would cluster the nodes based on similarity behavior and distance among the number of nodes. Optimal cluster head selection is done in terms of increased network lifetime. Secured data communication is guaranteed by introducing signature-based authentication procedure which would establish the secured communication medium between sender and receiver.

3.1 Optimal Edge Disjoint Routing Using Hybrid Genetic PSO Algorithm

The proposed algorithm SEDRP would select the mutually non interfering multiple paths from the set of route paths p that are constructed from the RREP cache to reach the destination successfully. Here the non interfering paths are defined as the multiple paths that share no common nodes among them. Many single paths can be integrated together to form the path if they don't have any common node with the (i) alternate route paths and (ii) set of neighbor nodes of all paths. The optimal route path would be chosen from the set of multiple non interfering route paths selected which are then placed in the active routing table to support the further data transmission. Remaining route paths other than selected

optimal route paths would be stored in the passive routing table which are then utilized in situation where the path failure occurs. Here the route path would be sorted in the ascending order to give them first preference in terms of size of the set of paths. That increased size of route path set can lead to optimal performance.

In traditional disjoint route construction procedures, first ever path discovered would be used for the routing purpose, while in the proposed procedure all the RREP packets select the most optimal route paths. This way of route path selection increases the chance of obtaining non-interfering multiple route paths. The proposed method ensures the reduced end-to-end delay outcome by initializing the process the non-interfering path selection process after data initialization. Here the parallelization of multiple non- interfering paths would be initialized after getting approval from the node architecture in order to optimize the network. Simply, this algorithm chooses the most optimal route path by considering all the RREP packets received instead of depending the first discovered route path. In this research work, optimal route path selection is performed by introducing the Hybrid genetic PSO algorithm under consideration of various performance metrics namely energy consumption, available bandwidth, and delay. These parameters are calculated as like as follows:

Available Bandwidth (BW): It is defined as the remaining bandwidth capacity found in the link between the sender node to the destination node present in multicast tree.

Available Power (P): It is defined as the remaining power of each node present in the multicast tree which is calculated as follows:

$$P = P_{\text{Total}} - E_{\text{consumed}} \tag{1}$$

where, P_{Total} defined as total available energy of node before data transmission which is assigned initially for every node in the network.

Available Delay (D): It is defined as the total time consumed to chose the optimal route path in order to ensure the successful data transmission.

3.2 Secured DATA Communication Using Signature-Based Authentication

This work aims to provide a secure environment for exchanging messages while conserving the limited resources of the sensors. The secured communication medium is between sender and receiver.

Secure communication procedure using signature-based authentication:

1. g is a cyclic subgroup of fq this is generated by the time p with high order n and identity detail o. and allow $h : 0, 1^*$ is a collision resistant characteristic

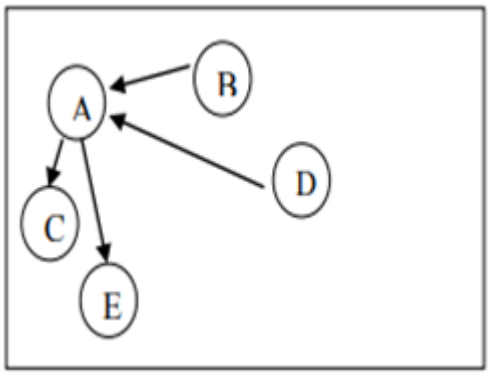

Fig. 1: Network example

2. Setup: singer a will pick a random integer d from $[1, n-1]$ then calculate the general public key $q = dp$ so as to be published while d is kept as a mystery.
3. Generate signature: a will use the non-public d to sign and it will generate (r, s) for message m in zero, 1^*
   (a). pick a random integer k in $[1, n-1]$, then compute $r = kp$ and take the x-coordinate of r that is, r
   (b). compute $s = okay - 1(e + dr) \mod n$, where $e = h(m)$.
   (c). if r, s in $[1, n-1]$, return (r, s); else, go to step 3(a)
4. verifying the signature. after receiving the message m in zero,1* and the signature (r, s) from a, a verifier b verifies the signature the use of a's public key q.
   (a). test that r, s in $[1, n-1]$. if any fails, return "reject signature".
   (b). compute $r0 = s - 1(ep + rq)$ wherein $e = h(m)$.
   (c). test the x-coordinate of r' is equal to r. if succeeds, go back 'be given signature'; else, return "reject signature".

In Fig. 1, B and D agree with A additionally, A trusts C and E. whilst B wants C's public key. A will sign on C's public key and broadcast it. Once it is skipped B acquire the signature B will confirm A's signature if it is skipped then it will launch one scalar product. D can use it if it trusts A so now B and D can accept as true with C (transitive).

4 Results and Discussion

In this section, the proposed algorithm (SEDRP) is compared with the existing CSDA-IRS [15], CTCM [16], DCWA and cocowa technique by plotting (using NS2) various simulation parameters. The parameters considered for simulation are shown in Table 1.

Performance Parameters

1. End-to-end Delay
2. Network Lifetime

Table 1: Simulation parameters

Network Size	100×100
Number of Nodes	250
Nodes Energy	0.5 J
BS location	(50,50)
Packet size	4000 bits
E	50 nJ/bit

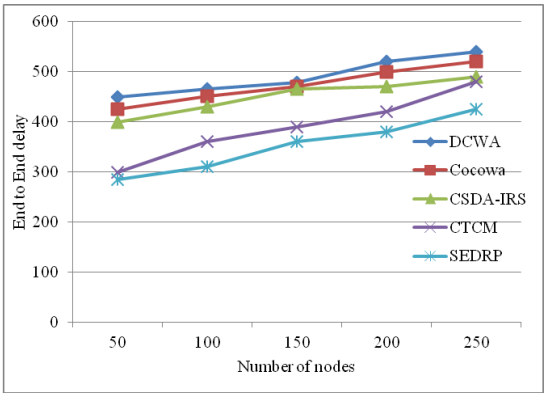

Fig. 2: End-to-End delay comparison

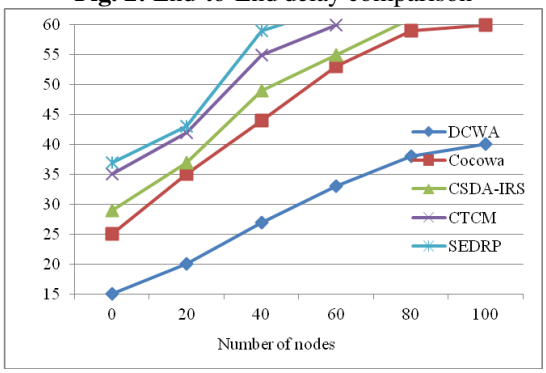

Fig. 3: Network lifetime comparison

3. Throughput
4. Packet Delivery Ratio
5. Packet Loss Ratio

The simulation results based on several simulation parameters are shown in Figs. 2 to 6.

End-to-end delay denotes the time taken for transmitting the packet from source to destination throughout a community. The transmission is commonly caused because of queuing and retransmission thanks to collision. From Fig. 2 it is shown that the end-to-end delay are better by way of the use of SEDRP technique. for this reason, it could be deduced that the green detection is done by using proposed method and the consequences concludes the advanced performance of the proposed method.

Lifetime refers to the time required with the aid of the network to perform until the primary sensor node or the group of nodes within the community runs out of strength. Fig. 3 represents the assessment of present and

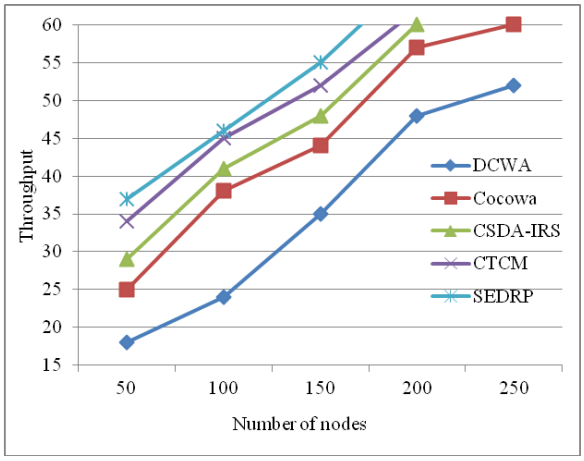

Fig. 4: Throughput comparison

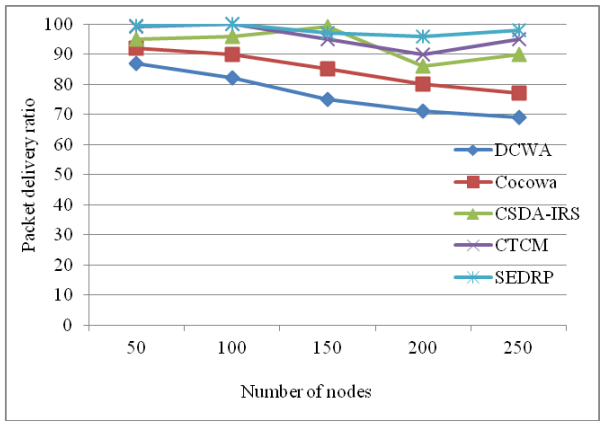

Fig. 5: Packet delivery ratio comparison

proposed device in terms of network lifetime metric. As a result, the green detection done with the help of the proposed approach proves to offer superior performance.

Throughput denotes the standard ratio of a success packet delivery over a message channel. The community throughput is measured in bits in keeping with 2nd (bit/s or bps) and the better throughput signifies the better performance. From Fig. 4, the comparison of the existing and proposed approach is observed. The SEDRP technique has shown lesser throughput. The proposed SEDRP system has proven expanded throughput value. The proposed method indicates the efficient detection and the consequences conclude that proposed machine shows better overall performance than the existing methods.

Packet delivery ratio is defined as the number of packets which has successfully reached the destination. Fig. 5 represents the overall performance comparison of current and proposed system in terms of packet delivery ratio. The existing approach exhibits the decrease values of packet transport ratio. But, the proposed SEDRP technique has shown vast increase in the packet transport ratio.

Table 2: Simulation Performance Comparison

METRICS	SEDRP	CTCM	CSDA-IRS	Cocowa	DCWA
Efficiency (%)	65–99	47–68	38–63	25–45	16–32
PDR (pkts)	23–93	18–55	16–49	15–33	5–27
Network life time (Secs)	56–87	56–87	26–67	10–47	23–40
End to end delay (msec)	32–11	62–15	58–0.29	78–47	98–76
Overhead (pkts)	11–19	12–25	10–21	26–47	37–78

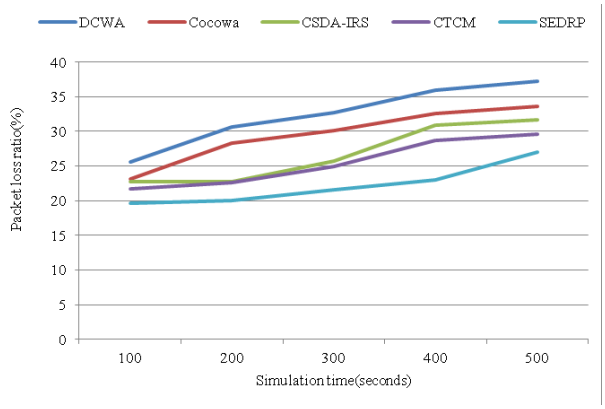

Fig. 6: Packet loss ratio comparison

Packet loss ratio denotes the percentage of packets lost during the transmission in the VoIP. Fig. 6 shows that the proposed SEDRP achieves less packet loss ratio than the existing methods. The various simulation parameters and comparison are shown in Table 2. From these simulation results, the proposed system SEDRP has best routing performances compared to existing systems.

5 Conclusion

In the proposed research method, these issues are resolved by introducing the Secured Edge Disjoint Routing Protocol (SEDRP). In the optimal edge disjoint routing is done by introducing the various research techniques that can ensure the optimal forwarding of the data packets. In this work, clustering is done in order to ensure the optimal and reliable data transmission which is done by using density aware optimal clustering approach. Secured data communication is guaranteed by introducing signature-based authentication procedure which would establish the secured communication medium between the sender and the receiver. The overall simulation evaluation is carried out in NS2 simulation environment from which it is proved that the proposed research method can enhance the routing performance in terms of increased packet delivery ratio. In future, it enhances with multipath secure routing.

References

[1] Z. Ghassemlooy, S. Arnon, M. Uysal, Z. Xu, and J. Cheng, Emerging optical wireless communications-advances and challenges. IEEE Journal on Selected Areas in Communications, vol. 33, no. 9, 1738–1749 (2015).

[2] J. Zhang, J. Tang, T. Wang, and F. Chen, Energy-efficient data-gathering rendezvous algorithms with mobile sinks for wireless sensor networks. International Journal of Sensor Networks, vol. 23, no. 4, 248–257 (2017).

[3] S. Lin, F. Miao, J. Zhang, G. Zhou, L. Gu, T. He and G.J. Pappas, ATPC: adaptive transmission power control for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), vol. 12, no. 1, 6. (2016).

[4] N. Javaid, M. Shah, A. Ahmad, M. Imran, M.I. Khan, and A.V. Vasilakos, An enhanced energy balanced data transmission protocol for underwater acoustic sensor networks. Sensors, vol. 16, no. 4, 487 (2016).

[5] C.N. Bailey, US Patent No. 9,742,724. Washington, DC: US Patent and Trademark Office (2017).

[6] B. Chen, Y. Qiao, O. Zhang, and K. Srinivasan, Air express: Enabling seamless in-band wireless multi-hop transmission. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (pp. 566–577). ACM, (2015).

[7] K. Chelli, Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the World Congress on Engineering, vol. 1, pp. 1–3 (2015).

[8] R.K. Sharma and D.B. Rawat, Advances on security threats and countermeasures for cognitive radio networks: A survey. IEEE Communications Surveys & Tutorials, vol. 17, no. 2, 1023–1043 (2015).

[9] R. Perlman, C. Kaufman and M. Speciner, Network security: private communication in a public world. Pearson Education India, (2016).

[10] S. Banerjee and S. Khuller, A clustering scheme for hierarchical control in multi-hop wireless networks, In: Proc. of Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Anchor-age, vol. 2, pp. 1028–1037 (2001).

[11] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on wireless communications, vol. 1, no.4, pp. 660–669 (2002).

[12] K. Vinoth Kumar, T. Jayasankar, V. Srinivasan and M. Prabhakaran, EOMRP: Energy Optimized Multipath Routing Protocol for Wireless Sensor Networks International Journal of Printing, Packaging & Allied Sciences, ISSN: 2320–4387 (Online), vol. 4, no. 1, pp. 336–343 (2016).

[13] S. Yi, J. Heo, Y. Cho and J. Hong, PEACH: power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks, Computer Communications, vol. 30, pp. 2842–2852 (2007).

[14] R.J. Kavitha and B. Elizabeth Caroline, PROXUM: An Energy and privacy aware data aggregation in HWSN,

International Journal of Advances in Natural and Applied Sciences, vol. 9, no. 6, pp. 316–322 (2015).
[15] R.J. Kavitha and B. Elizabeth Caroline, Hybrid Firefly and Identity-Based Ring Signcryption Scheme Based Secure Data Aggregation for Clustered Heterogeneous Wireless Sensor Network, Transylvanian Review, vol. 24, no. 7, pp. 841–851 (2016).
[16] R.J. Kavitha and B. Elizabeth Caroline, Secured Reliable Data Transmission on Multi Hop Wireless Sensor Networks, Journal of Cluster Computing, (2017)

R. J. Kavitha is working as Assistant Professor, Department of ECE in University College of Engineering, Panruti (A Constituent College of Anna University, Chennai) since Aug 2009. She obtained B.E. in Electronics & Communication Engineering from Govt. College of Engineering, Salem in 1998, M.E. Optical Communication from A.C. College of Engineering & Technology, Karaikudi in 2007 and Ph.D. in Sep 2017 from Anna University. Her area of specialization is Wireless Sensor Networks, Digital Communication and Medical Electronics. She has 17 years of teaching experience. She has organized many events such as workshops, seminars, FDP, Symposiums. She has visited several countries like Qatar, Malaysia, Singapore.

N. Satheesh is currently working as Associate Professor in Chalapathi Institute of Engineering & Technology, Guntur. He received his Ph.D., CSE, Karpagam University, Coimbatore. And completed M.E., CSE, Annamalai University, Chidambaram. And completed B.E., ECE. Over all 13+ years of experience, 10+ years in teaching as an Associate Professor in Computer science stream handling a various software skills, technologies and driving my students towards innovation in the field of IT, and 2+ as a Software Engineer in Computer Science stream handling a various software International Journal Publication 04 International Conference: 04