International Journal of Engineering

Journal Homepage: www.ije.ir

Evolutionary Computing Assisted Wireless Sensor Network Mining for QoS-Centric and Energy-efficient Routing Protocol

R. Sunitha*[a], J. Chandrika[b]

[a] *PES University, Bangalore, India*
[b] *Malnad College of Engineering, Hassan, India*

PAPER INFO

Paper history:
Received 30 December 2019
Received in revised form 27 January 2020
Accepted 06 March 2020

Keywords:
Wireless Sensor Network
Network Mining
Evolutionary Computing
Network Optimization
Malicious Node Detection
Link-connectivity-availability
Dynamic Routing

ABSTRACT

The exponential rise in wireless communication demands and allied applications have revitalized academia-industries to develop more efficient routing protocols. Wireless Sensor Network (WSN) being battery operated network, it often undergoes node death-causing pre-mature link outage, data drop and retransmission causing delay and energy exhaustion. Furthermore, the presence of a malicious node to impacts network performance adversely. In this paper, a highly robust and efficient Evolutionary computing assisted WSN routing protocol is developed for QoS and energy-efficiency. Our proposed routing protocol encompasses two key functions Network Condition Aware Node Profiling and Malicious Node Detection (NCAMND) exploits or mines the dynamic node/network parameters to identify malicious node, and Evolutionary Computing assisted Dual-Disjoint Forwarding Path (EC-DDFP) model learns over node/network connectivity and availability information to obtain a dual-disjoint path with no-shared components to ensure QoS centric and energy-efficient routing. Simulation results affirm that the proposed routing protocol achieves higher throughput, low energy consumption, and low delay that confirm its suitability for real-time WSN systems.

***doi**: 10.5829/ije.2020.33.05b.10*

1. INTRODUCTION

The exponentially rise in wireless communication systems and allied applications have revitalized academia-industries to develop a more efficient and robust routing protocol to meet up surging demands. Contemporarily, the modern human life can't be imagined without communication system where each stakeholder intends to exploit known and unknown information to make an optimistic decision by sharing information from one peer to another.

Exploring in-depth it can be found that the predominant challenges of QoS assurance in WSN are caused due to dynamic network nature, link-outage, congestion, topology change [1] (it has gained wide-spread attention across academia-industries due to its low-cost transmission timely-solution nature), delay, malicious nodes, etc [2]. However, these facts reveal that the lack of node and network awareness can be the prime reason for such QoS compromise. In other words, a robust network awareness model and information exchange across the IEEE 802.15.4 protocol stack can enable dynamic network sensitive routing decisions [1-5]. Furthermore, WSN being a cooperatively operating protocol often undergoes adversaries due to the presence of the malicious node that often intends to mislead routing decisions, drop packets, and deny services causing data loss, retransmission, delay, QoS-violation and energy-exhaustion" [1-5]. On the other hand, the false information provided by a smart (intruder) node too can force the network to undergo link-loss or packet loss causing QoS degradation and energy-exhaustion. In such a case, learning network pattern, dynamic parameters, mining node as well as network conditions continuously and making strategic path planning can be vital to yield energy-efficiency as well as QoS provision. To achieve it

*Corresponding Author Institutional Email: *sunithar1389@gmail.com* (R. Sunitha)

Please cite this article as: R. Sunitha, J. Chandrika, Evolutionary Computing Assisted Wireless Sensor Network Mining for QoS-Centric and Energy-efficient Routing Protocol, International Journal of Engineering (IJE), IJE TRANSACTIONS B: Applications Vol. 33, No. 5, (May 2020) 791-797

learning or mining both dynamic node/network parameters as well as node-trustworthiness over an operating period can be vital [1-4].

Considering above stated factors, in this paper we have developed a highly robust Evolutionary Computing (EC) assisted routing protocol for dynamic network-aware routing decisions in WSNs. In this paper, we emphasize dynamic network monitoring and node/network pattern mining over the operating period to identify malicious node and isolate it to preserve optimal (network) network efficiency. Evolutionary Computing (EC) based dual-disjoint path formation mechanism that intends to obtain two optimal forwarding paths with "no common components or nodes". To achieve it, a well-known heuristic or EC algorithm named Genetic Algorithm (GA) has been applied that mines over the dynamic network/node parameters and identifies malicious nodes to obtain fault-resilient dual-disjoint best forwarding paths for QoS-centric transmission. EGA exploits the above-stated parameters to obtain dual disjoint paths with minimum connected nodes or components and high node reliability (high availability, low connection-loss). Here, the prime objective is to introduce two disjoint best forwarding paths which could enable swift data transmission to the destination, without imposing iterative node-discovery in case of (future) node-death. This approach not only strengthens transmission reliability but also alleviates energy consumption due to iterative network discovery and hence achieves maximum possible QoS provision with high transmission reliability and low energy consumption. Our proposed routing protocol has been developed using Network Simulator Ver-2 (NS2) and performance has been examined in terms of packet delivery ratio, packet loss, energy consumption, etc.

The remaining sections of the presented manuscript are divided as follows. Section II discusses related work, which is followed by research questions in Section III. Section IV presents the problem formulation, while the overall proposed system and its implementation are discussed in Section V. Section VI presents the simulation results and allied inferences, while the overall conclusion is given in Section VII. References used in this research are given at the end of the manuscript.

2. RELATED WORK

This section primarily discusses some of the key literature about the targeted research objective of designing robust outlier identification and optimal routing protocol for WSNs. Noticeably, in the majority of the existing approaches above stated objective is dealt in two distinct approaches, first outlier detection, and second routing optimization. Unlike these approaches, we focus on developing a robust integrated solution to meet QoS as well as energy-efficiency demands. Zhang et al. [6] focused on exploiting both node credibility and time-series analysis approach to detect outliers for better routing decisions in dense WSN to be applied in urban network conditions. Authors have applied the Bayesian model to obtain the reputation value for each participating node which has been compared with a defined threshold range to classify a node as malicious or outlier. A similar approach was developed by Sutaone et al. [7], where considering the threat of malicious node selection as cluster head (CH); authors developed Trust-based Cluster head Validation and Outlier Detection Technique for Mobile Wireless Sensor Networks (TCVOD). In their approach, at first, CH's cumulative trust score was obtained and adaptive CH selection or rejection scheduling was performed. Abid et al. [8] applied inter-node distance data for outlier detection. Though, such approaches can be suitable for fixed topology with zero variation probability; however, classifying a node based on merely inter-node distance can't be a suitable solution. To exploit multiple parameter based outlier detection, authors have applied machine learning methods [9]. Kumar et al. [9] applied the Bayesian Network model to estimate the conditional dependency amongst the nodes in the network to identify malicious nodes. Xu et al. [10] proposed a support vector machine and K-Nearest neighbor (SVM-KNN) model to perform outlier detection in WSN. The authors used KNN to obtain network statistics amongst the neighboring node, while SVM was applied as a spatial-temporal classifier to detect malicious or outlier node. Martins et al. [11] developed a multi-agent model for outlier detection in WSN. To achieve it, authors applied dynamic time-series network data which was learned using Least Squares SVM (LS-SVM) to detect outlier identification. Liu et al. [12] proposed a knowledge driven training based adaptive routing concept, where at first alternating minimization concept was applied to perform outlier detection, which was followed by a link-level context-aware rate adaptation system for routing decision. However, the maximum throughput by the network was obtained as 87%. Yu et al. [13] applied a recursive Principle component analysis (PCA) based outlier detection approach for IoT ecosystems. This approach was a cluster-based model that collects the redundant data and learning over respective entity-wise significance identifies outlier node. However, the efficacy of such a system in a real-time dynamic sensing environment remains suspicious [14]. Feng et al. [15] applied a node's credibility feedback based distributed outlier detection system for WSN. Though authors tried exploiting Bayesian-based credibility estimation to perform outlier detection, it is highly complex and suspicious under dynamic topology which is common in contemporary network conditions. Zhang et al. [16] designed an approach by amalgamating network

surveillance, unique message or fake message identification and different spatio-temporal correlation and consistency. These multiple parameters performed malicious node ident.

3. PROPOSED SYSTEM

This section primarily discusses the overall propose d systems and its systematic implementation. As already stated, this research primarily intends to exploit the efficacy of the robust network condition awareness in conjunction with dynamic node/network mining for optimal routing decisions. The overall research contribution can be summarized into two key forms:m

3. 1. Network Condition Aware Node Profiling and Malicious Node Detection (Ncamnd) This section primarily discusses the key node parameters and their use for malicious node detection and routing decision. Considering the behavioral characteristics of the malicious node in the contemporary WSN environment where a node might mimic the genuine node by transmitting false information, in our proposed NCAMD model both behavioral as well as statistical parameters are considered. Some of the key parameters obtained in our proposed model and its inferences towards QoS and energy-centric routing is given as follows.

3. 1. 1. ***Irregular IEEE 802.15.4 MAC Inform*** During communication, a WSN node might undergo continuous changes in topology. In addition, it can also undergo dynamism due to congestion, dead-nodes, link-outage, etc causing data drop at IEEE 802.15.4 MAC layer at the transmitter. In general, the predominant reasons behind data drop at 802.15.4 MAC are congestion and out-of-range conditions. Usually, such data drops take place due to lack of information at the transmitter and hence the availability of proper information at the transmitter, which can be availed by the forwarding node can be vital for QoS centric routing decision. Malicious nodes often provide misleading or false MAC information that causes packet loss, and therefore identifying such packet loss and irregular MAC information a node can be identified as malicious or intruder. With this motive, in this paper, we have applied this node/network parameter as one of the key signifiers for malicious node detection.

Thus, employing or mining the obtained reliability and the link-quality between two nodes the forwarding path is decided. In our proposed routing model, the probability of successful delivery by a node at the IEEE 802.15.4 layer is obtained using Equation (1).

$$P_M = \frac{\xi_{Rx(t_{i-1},t_i)}}{\xi_{Exp(t_{i-1},t_i)}} \quad (1)$$

In Equation (1), ξ_{Rx} states the total number of beacon message received, while, while ξ_{Exp} presents the total expected beacons during (t_{i-1}, t_i) time period.

3. 1. 2. Queuing Overflow Exploiting nodes queuing delay or allied congestion information certain misbehaving nodes or malicious nodes can be identified to avoid its participation in forwarding path formation. Inheriting this feature, in our proposed model we have identified the malicious node by examining or learning over the traffic data intensity of the participating nodes. In our applied method, the transmitter node monitors and collects the load-traffic statistics of the connected neighboring nodes. Here, to obtain load-condition and congestion of each candidate node, we estimated interface queue length at the MAC layer and broadcasts it as ACK to the neighboring node. Let, i be the one-hop distant sensor node, while l_j be the jth sample value signifying queue length at a certain time instant. Now, with L as the total queue length samples over a simulation period, we obtained the average traffic load at a node using Equation (2).

$$T_{load\_i} = \frac{1}{L}\sum_{j=1}^{N} l_j \quad (2)$$

Now, l_{max} as the highest queue length of a node (at MAC layer), the total traffic density at a node is obtained using Equation (3).

$$T_{loadDens\_i} = \frac{T_{load\_i}}{l_{max}} \quad (3)$$

In NCAMND the dynamic value of $T_{loadDens\_i}$ have been mined or learned to obtain the probability of successful transmission by a node, P_{Succ_i} , as given in Equation (4).

$$P_{Succ\_i} = \left[1 - T_{loadDens\_i}\right] \quad (4)$$

As P_{Succ_i} is directly related to the transmission delay and energy-exhaustion, our proposed routing protocol considers the significantly small value of TLD and hence only a node with small TLD has been considered for forwarding path selection.

3. 2. Evolutionary Computing Assisted Dual-disjoint Forwarding Path (EC-DDFP) Once performing the malicious node detection, our proposed routing protocol intends to avoid detected malicious nodes and executes a novel DDFB selection to deliver data reliably. As a novel solution, our proposed EC-DDFB model employs dual objective function where the first intends to achieve the optimal forwarding nodes for path planning, while other functions to achieve best dual-disjoint forwarding path estimation for reliable transmission. Considering these two hypotheses, we have applied a robust EC variant named GA that intends to achieve the above-stated statements for QoS-centric communication. Noticeably, maintaining low-hop

counts, high connectivity (low-connectivity loss) and high availability with minimum shared components for QoS centric communication. The detailed discussion of the proposed EC-DDFP model is given as follows.

3. 2. 1. GA based DDFP and Network Optimization

As stated in previous sections, our proposed EC-DDFP model exploits the above discussed link-connectivity and availability parameters to obtain the optimal set of DDFP to enable reliable transmission. As the objective function, EC employs the link-connectivity loss parameter (17) as the cost function to obtain a set of DDFP. Here, the EC model intends to maintain DDFP with minimum or no shared components by obtaining proper forwarding paths by exploring or mining over the search space containing a set of all feasible paths. This process is continued and the eventual DDFP is constructed by adding a new hop sensor node by obtaining its connectivity probability values. Thus, this mechanism continues until the probability of obtaining better paths becomes very low. The overall process of the targeted network optimization comprises two phases, DDFP path selection, and pruning. The detailed discussion of these mechanisms is given as follows. Identifying a reliable path for certain iteration k can eventually alleviate the presence of other paths from S_k having low-cost function or the connectivity and/or availability. This, as a result, can not only achieve QoS centric routing but can also reduce computational cost and energy consumption. To achieve it, our proposed EC based model estimates a function called "Cost-Function $c(\mathcal{P})$" for each possible path $\mathcal{P}$. Thus, the optimal set of paths is obtained using Equation (19).

$$\mathcal{P}^* = arg\min_{R} c(\mathcal{P}) \tag{19}$$

Now, to estimate the cost function$c(\mathcal{P})$, we implement the following mechanism. Consider $\bar{\mathcal{P}}$ is one of the connecting link or forwarding path constituted by extending R, an incomplete path using a suitable link with zero-unavailability. Noticeably, in this configuration, the path R is connected to the node n_f. Thus, for any complete forwarding path $M_i \in S_k$, consider that $L(\bar{\mathcal{P}}, M_i)$ be the connectivity-loss for the source or the starting node n_0. Then, the average connectivity loss can be obtained as Equation (20).

$$\tilde{L}(\mathcal{P}) = \frac{1}{N_c}\sum_{i=1}^{N_c} L(\bar{\mathcal{P}}, M_i) \tag{20}$$

Realizing the fact that the link-loss increment can be an unavoidable component under dynamic network scenario for a path $\mathcal{P}$, we reformulate cost function (20) as (21).

$$c(\mathcal{P}) = \tilde{L}(\mathcal{P}) + E(\mathcal{P}) \tag{21}$$

Noticeably, in Equation (21), the second component $E(\mathcal{P})$is calculated based on the average loss incurred per link on the complete path pairs. Mathematically,

$$E(\mathcal{P}) = \frac{1}{N_c}\sum_{i=1}^{N_c} E(\mathcal{P}, M_i) \tag{22}$$

where

$$E(\bar{\mathcal{P}}, M_i) = \frac{\tilde{L}(M_i)}{\lambda} d\left(n_{\mathcal{P}}, n_f\right) \tag{23}$$

To obtain such distance values, Graph theory concept has been applied stating that for a Graph matrix A, with different components a_{ij} where $a_{ij} = 1$ when the link between node i to node j is active, else $a_{ij} = 0$ and $a_{ii} = 1$. With such conditions, we obtain matrix $B(k)$ as per Equation (24).

$$B(k) = \mathbb{A}^k \tag{24}$$

In Equation (24), $B(k)$ has the components $b_{ij}(k)$ which are equivalent to the total number of paths to reach i to j with the number of hops lower than k. In this case, with $b_{ij}(k) = 0$ there can't be any possible path reaching i to j in k-hops. Thus, we obtained the distance from node i to node j as the shortest path, which is obtained using Equation (25).

$$d(i,j) = \min_{b_{ij}(k)>0}\{k\} \tag{25}$$

Equation (25) signifies that the value of $d(i,j)$ can be the smallest value of the hops k with $b_{ij}(k) > 0$.

4. RESULTS AND DISCUSSION

Considering, the exponentially rise in the significance or use of WSN networks for different contemporary demands including IoT ecosystems and M2M communication, this research mainly focused on enhancing QoS provision and energy-efficiency. To achieve it, we formulated a solution by considering key hypotheses. First states that identifying malicious node or outlier entity from WSN sensor nodes by exploiting dynamic node and/or network parameters can help to avoid packet loss probability and retransmission so as to avoid energy-exhaustion. Unlike major conventional researches where authors have applied classical distance parameters such as Dijkstra or Euclidean distance to perform routing decisions, we applied a well known EC algorithm named Genetic Algorithm (GA) which exploited link-availability and connectivity information to perform optimal DDFP formation. Thus the strategic implementation of NCAMND and EC-DDFP model enabled reliable and QoS centric data transmission over WSNs. Noticeably, the identification of malicious node reduced the probability of packet drop while DDFP ensured that even in case of any probable link loss or node-death the proposed routing protocol can ensure timely data delivery without imposing retransmission and iterative node discovery. This approach achieved both QoS assurance as well as energy efficiency. The overall proposed WSN routing model was developed using the NS2 development platform. A snippet of the simulation variables and allied experimental setup values are given in Table 1.

As discussed in the previous section, as eventual solution obtaining the link-loss probability and distance information, our proposed EC-DDFP model achieves a (dual) set of best forwarding paths to perform data transmission between the source and the destination. To examine the efficiency, we have compared the performance of the proposed with a recently proposed evolutionary computing named Cuckoo Search and Harmony Search (HS) based routing protocol for WSN [33]. Noticeably, unlike our proposed routing where both outlier neutralization, as well as optimal routing decision, is considered as an eventual goal, Improved Cuckoo Search.

We find that the proposed routing model exhibits low loss as compared to the iCSHS protocol (Figure 1).

Figure 3 exhibits the delay incurred in both approaches. As already indicated, the iCSHS model at first applies the Cuckoo search to perform clustering optimization, which is then followed by HS based routing decision where it performs two-stage iterative node and path verification. This overall process increases latency, which can be visualized by Figure 2. On the contrary, our proposed routing protocol obtains network parameters dynamically and updates the same as a proactive manner. As stated, the iCSHS model is the computationally exhaustive approach and hence is supposed to incur high energy consumption during clustering optimization and subsequent path planning. It makes iCSHS to undergo high energy consumption. On the contrary, our proposed model preserves energy contributed due to low or reduced computational complexity and retransmission probability (Figure 3).

TABLE 1. Experimental Setup Values

Parameter	Value
Number of nodes	60
Network dimension	100 × 100
Radio	200 meters
Tx-Rate	10-512 p/s
Career frequency	2.5 GHz
Antenna type	Omni directional
Efficiency of RF power amplifier	0.47
Link margin	40 dB
Gain factor	30 dB
Power density of radio channel	-130 dBm /Hz
Noise Figure (Receiver)	10 dB
BER performance	10^{-3}
Transmitter circuit power consumption	98.2 mw
Antenna gain	5 dB
Packet size	512 kb
EC-GA Parameter Stopping Criteria	Adaptive
Objective function	Link-loss probability

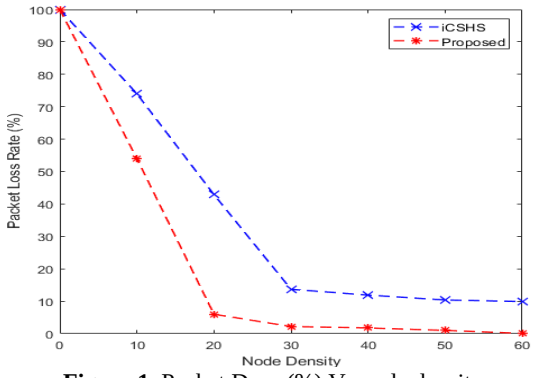

Figure 1. Packet Drop (%) Vs node density

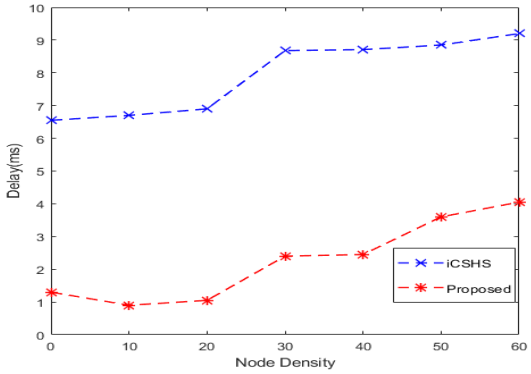

Figure 2. End-to-End delay Vs node density

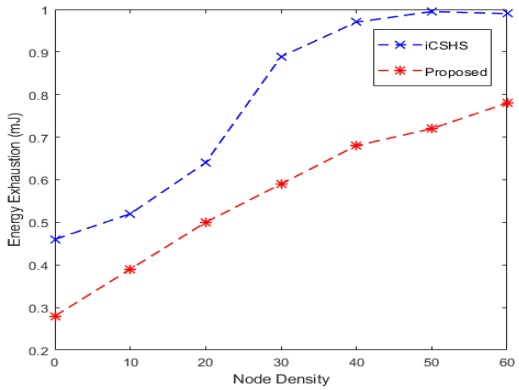

Figure 3. Energy exhaustion or consumption Vs node density

5. CONCLUSION

Realizing the fact that in even being one of the most employed wireless network solutions, WSNs often undergo adverse conditions like node-death, pre-mature link-outage, topological variations, etc. In this paper, an overall implementation was split into two concurrently functional models. The first model of the proposed system, i.e., NCAMND exploited multiple dynamic parameters such as irregular MAC information exchange,

queuing overflow, probability of the successful data delivery, etc to identify a malicious node. The second model to achieve fault-resilient transmission objective a well known Evolutionary Computing algorithm was developed named Genetic Algorithm which exploited network and node connectivity and link availability to perform Dual Disjoint Forwarding Path (DDFP) estimation. Network Simulator based simulation revealed that the proposed routing protocol achieves higher throughput, low packet loss and high energy-efficiency with native IEEE 802.15.4 protocol standard and hence follows backward compatibility. It makes the proposed system suitable for real-time routing solutions. In the future, based on network dynamism spatio-temporal features can be obtained and different classifiers or machine learning methods can be applied to exploit inter-relation amongst spatial as well as temporal behavior of nodes to detect malicious node. The malicious patterns can be converted as knowledge to enable time-efficient routing decisions in future steps, without iterating the same detection process.

6. REFERENCES

1. Ehsan, S. and Hamdaoui, B., "A survey on energy-efficient routing techniques with qos assurances for wireless multimedia sensor networks", ***IEEE Communications Surveys & Tutorials***, Vol. 14, No. 2, (2011), 265-278.
2. de Araújo, G.M. and Becker, L.B., "A network conditions aware geographical forwarding protocol for real-time applications in mobile wireless sensor networks", in 2011 IEEE International Conference on Advanced Information Networking and Applications, IEEE. (2011), 38-45.
3. Ezdiani, S. and Al-Anbuky, A., "Modelling the integrated qos for wireless sensor networks with heterogeneous data traffic", ***Open Journal of Internet Of Things***, Vol. 1, No. 1, (2015), 1-15.
4. Spachos, P., Toumpakaris, D. and Hatzinakos, D., "Qos and energy-aware dynamic routing in wireless multimedia sensor networks", in 2015 IEEE International Conference on Communications (ICC), IEEE. (2015), 6935-6940.
5. Sen, J. and Ukil, A., "An adaptable and qos-aware routing protocol for wireless sensor networks", in 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, IEEE. (2009), 767-771.
6. Zhang, H. and Li, Z., "Anomaly detection approach for urban sensing based on credibility and time-series analysis optimization model", ***IEEE Access***, Vol. 7, (2019), 49102-49110.
7. Sutaone, M., Mukherj, P. and Paranjape, S., "Trust-based cluster head validation and outlier detection technique for mobile wireless sensor networks", in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE. (2016), 2066-2070.
8. Abid, A., Kachouri, A. and Mahfoudhi, A., "Anomaly detection through outlier and neighborhood data in wireless sensor networks", in 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), IEEE. (2016), 26-30.
9. Dwivedi, R.K., Pandey, S. and Kumar, R., "A study on machine learning approaches for outlier detection in wireless sensor network", in 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE. (2018), 189-192.
10. Xu, S., Hu, C., Wang, L. and Zhang, G., "Support vector machines based on k nearest neighbor algorithm for outlier detection in wsns", in 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE. (2012), 1-4.
11. Martins, H., Januário, F., Palma, L., Cardoso, A. and Gil, P., "A machine learning technique in a multi-agent framework for online outliers detection in wireless sensor networks", in IECON 2015-41st Annual Conference of the IEEE Industrial Electronics Society, IEEE. (2015), 000688-000693.
12. Liu, H., He, J., Rajan, D. and Camp, J., "Outlier detection for training-based adaptive protocols", in 2013 IEEE Wireless Communications and Networking Conference (WCNC), IEEE. (2013), 333-338.
13. Yu, T., Wang, X. and Shami, A., "Recursive principal component analysis-based data outlier detection and sensor data aggregation in iot systems", ***IEEE Internet of Things Journal***, Vol. 4, No. 6, (2017), 2207-2216.
14. O'Reilly, C., Gluhak, A., Imran, M.A. and Rajasegarar, S., "Anomaly detection in wireless sensor networks in a non-stationary environment", ***IEEE Communications Surveys & Tutorials***, Vol. 16, No. 3, (2014), 1413-1432.
15. Feng, H., Liang, L. and Lei, H., "Distributed outlier detection algorithm based on credibility feedback in wireless sensor networks", ***IET Communications***, Vol. 11, No. 8, (2017), 1291-1296.
16. Zhang, Y.-Y., Chao, H.-C., Chen, M., Shu, L., Park, C.-H. and Park, M.-S., "Outlier detection and countermeasure for hierarchical wireless sensor networks", ***IET Information Security***, Vol. 4, No. 4, (2010), 361-373.

Persian Abstract

چکیده

افزایش نمایی درخواست های مخابرات بی سیم و کاربرد های وابسته به آن سبب تجدید حیات صنعت و دانشگاه در گسترش مسیر یابی پروتکل های موثر شده است. شبکه حسگر بی سیم (WSN) که شبکه ای با تغذیه باتری است، اغلب متحمل مرگ گره می شود که سبب قطع زود هنگام ارتباط، افت داده، ارسال دوباره منجر به تاخیر و کاهش انرژی می شود. علاوه بر این، حضور گره معیوب نیز بر کار کرد شبکه تاثیرعکس می گذارد. در این مقاله یک پروتکل WSN مسیر یابی بسیار انعطاف پذیرو موثر به کمک محاسبات تکاملی به منظور QoS و بهره انرژی گسترش یافته است. پروتکل مسیر یابی ارائه شده دو کار کلیدی آشکار سازی گره معیوب و Network Condition Aware Node Profiling (NCAMND) را دور می زند تا با بهره برداری و یا نقب زنی پارامتر های گره/شبکه، گره معیوب را شناسایی کند. همچنین مدل مسیر پیشرو Dual-Disjoint با کمک محاسبات تکاملی (EC-DDFP) روشنگر اتصال گره/شبکه و در دسترس بودن اطلاع می باشد تا یک مسیر Disjoint–Dual بدون مولفه های مشترک بدست آید و QoS متوسط و مسیری با بهره وری از نظر انرژی تضمین شود. نتایج شبیه سازی نشان می دهند که پروتکل ارائه شده به خروجی بالاتر، مصرف انرژی کمتر، وتاخیر کمی دست می یابد که مناسب بودن آن را برای سامانه های WSN بی درنگ تایید می کند.