Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.138 – 143

RESEARCH ARTICLE

An Alternative M-Path Adaptive Routing Approach for WSN Optimization

Sandeep Kumar[1] (M.Tech Scholar)
Deptt. Of ECE PPIMT, Hisar, Haryana, India
Sandeepgoyat246@gmail.com

Nidhi[2] (Assistant Professor)
Deptt. Of ECE PPIMT, Hisar, Haryana, India
nidhibajag44@gmail.com

Abstract— Sensor Network is composed using smaller nodes with certain restrictions. To improve the network communication, it is required to optimize the communication route. In this work, instead of generating single communication path, multiple paths are generated to optimize the network communication. These M paths are selective alternatively so that the load on the path node will be distributed. This distributed load approach has reduced the energy consumption over the network and improve the network life. The simulation results show that the work has improved the overall energy consumption in the network.
Keywords: Distributed, M-Path, Optimized, Energy

I. INTRODUCTION

Sensor network is one of the critical network form defined for specialized networks. This network is defined using small tiny sensors applied in application specific scenario. The network nodes are defined under certain restrictions and constraints. These restrictions include limited sensing range, energy, memory and processing capability. The constraints are defined under specification of application, application area and the environment. Most of the sensor networks are defined under architectural behavior. This architecture is able describe all the relative requirements of the network. The architectural constraints are here defined under the requirement constraints and application specification. These constraints are applied to track the localization to the sensor nodes. Different network constraints are defined under the positional specification so that the network design and optimization will be done. The design constraints and objectives relative to the work are presented in this section.

Some of these sensor network characteristics are shown in figure 1

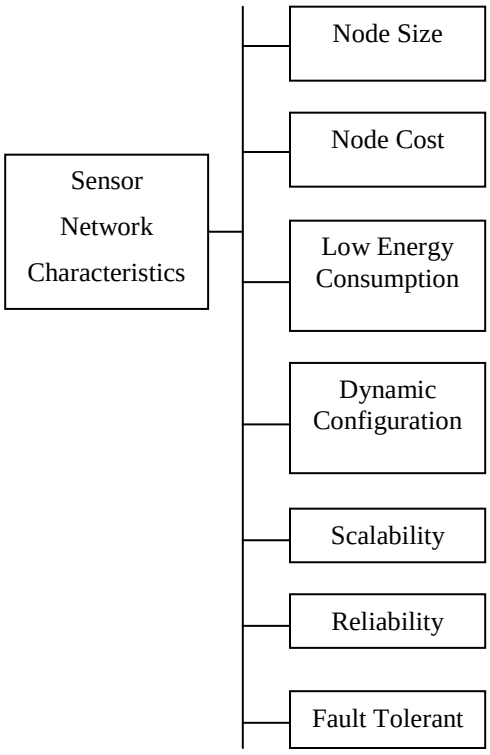

Figure 1: WSN Characteristics

The sensor network characteristics include the specification of physical constraints, network constraints and communication constraints. The physical attributes of nodes includes node size and cost vector. These cost vectors are depends on the cost limitation, probability vectors. Based on these criteria, the network configuration characteristics are formed. The design level, localization level and architectural level features are based on these specifications. These specifications also includes the identify the communication cost at node level. The architectural network constraints are defined with physical characteristics specification. Once the cost vector and initial constraints are defined, the next work is to define the network level constraints. These constraints are respective to the network scenario, application specification, and application area specification. The specifications of these constraints are relatively to the broader effect and present the network division criteria and specification of network area constraints. The protocol level constraints are defined in these criteria. At the final configuration constraints specification, the communication parameters are defined. These parameters include the communication frequency, type of data, type of communication etc. Once the communication characteristics are defined, the data communications, energy consumption respective to each communication are also specified. The communication control and the network life parameters are described under the network scenario. The communication constraints are effective optimize the network under process specification such as routing algorithm optimization, coverage optimization etc.

In this paper, route optimization adaptive model is provided to improve the network communication and network life. The defined model is based on the algorithmic approach optimization under constraint specification. In this paper, M-alternative paths are generated and used sequentially so that the load over the path nodes will be reduced and the optimized communication will be performed. In this section, the sensor network architecture is defined along with characteristics definition. These characteristics itself defines network constraints. In section II, the work defined by earlier researchers is discussed. In section III, the proposed research model is presented. In section IV, the results associated with this work. In section V, the conclusion of the work is presented.

II. RELATED WORK

WSN communication is one of the challenging research areas that require lot of optimization. This optimization is achieved at architecture level and algorithm level. Some of the work defined by earlier researchers at different levels is given in this section. Charlier Isaksson[1] has presented the work on network traffic analysis under risk reduction at different levels. Author defined the mining based approach to reduce the risk level in global environment. The risk vectors are here analyzed under DOS attack. The attack specification communication is provided to optimize the network communication and network strength. The work is defined to improve the scalability in the network so that the optimized network communication will be performed. Li Yao [2] has presented a configuration adaptive model to optimize the network communication. Author defined an energy loss adaptive communication so that the reliable communication will be performed. Author defined the attack adaptive approach for optimizing the network communication so that the reliable communication will be performed. Peyman Kabiri[3] presented a communication model under attack preventive approach so that the feature adaptive communication will be performed. The work model is defined to identify the network attack and to generate the preventive network path so that the communication over the network. Author defined the feature adaptive communication under honey pot communication so that the reliable communication will be held. Rahul Khanna[4] has provided a HMM based probabilistic approach for optimizing the communication so that the effective communication route will be formed. Author defined the analysis under response time so that the defensive network communication will be communication. Author defined the communication under communication behavior under multiple communication vectors so that the reliable route generation will be obtained. Author defined the frequency adaptive communication so that the effective route formation will be done.
Pengfan Yan [5] has presented the pattern generation model to secure the physical environment so that the reliable communication will be performed. Author defined the secure communication so that the access communication analysis so that the information tracking in the network. Author defined the reliable communication so that the effective network communication will be formed. Kapil Kumar Gupta [6] has provided a conditional probability based approach for defensive mechanism so that the random communication environment. Author defined the defensive communication model so that the safe communication will be performed. Author defined the task analysis and random conditional analysis so that the attack preventive mechanism will be performed. Author defined a mitigation model so that the reliable communication so that the reliable communication so that the information tracking so that the secure communication modeling will be done. Jaao B.D. Cabrera [7] has provided the classification and detection model under sequence mining approach for secure communication under dictionary modeling so that the substantial analysis so that the effective network communication will be performed. Author analyzes the communication and performed the attack count so that the reliable communication will be performed. Sandip Ashok Shivarkar[8] has defined the incidental aspect analysis so that the random field analysis so that the information communication will be performed. Author defined the threat violation analysis under accuracy strength formation so that the safe communication will be performed. Author defined the intrusion adaptive communication so that the communication violation will be performed under certain criteria. Author defined the analysis under multiple incident vectors to improve the communication strengths. Richard J. Bolton[9] defined fault adaptive model for statistical analysis so that the learning aspect based defect analysis will be performed. Author defined the attack preventive model for attack formation so that the route generation will be done. Ramkumar Chinchani[10] has presented the attack identification to provide realistic network communication under statistical approach. Author provided the safe communication in attacked network. Ping Yan [11] has defined has improved the communication behavior under the strength specification so that the clustered communication will be performed. K. Hanumantha Rao[12] has presented the clustered portioned model for optimizing the network communication in attack analysis so that the communication similarity analysis will be performed and the safe communication in the network will be performed.

III. RESEARCH METHODOLOGY

The presented work is here defined to optimize the sensor network communication under routing approach. The work is here defined in three sub stages. In first substage, the route optimized algorithm is defined. Instead of generating single optimized path, multiple i.e. M optimized paths are generated in this work. These generated paths are then applied between the same sources and sink alternatively. The sequential allotment of the network paths is done so that the load on each path node will be reduced and get distributed. This distributed path communication approach reduced the network communication and improved the network life. The broader work model is shown in figure 2.

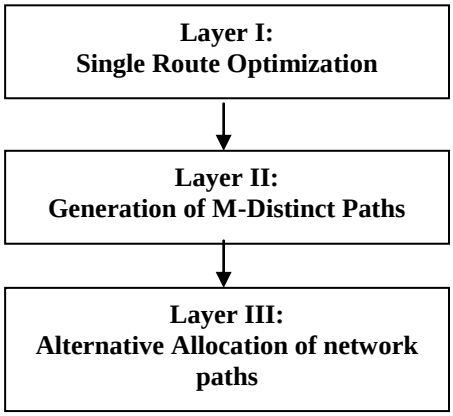

Figure 2: Layered Communication Model

A) Layer 1:

This layer is basically defined to generate the optimized network path. The path generation is here done under multiple vectors. The vectors considered for path generation includes distance analysis, energy analysis and sensing criteria analysis. The distance adaptive work model adapted in this work is shown in figure 3

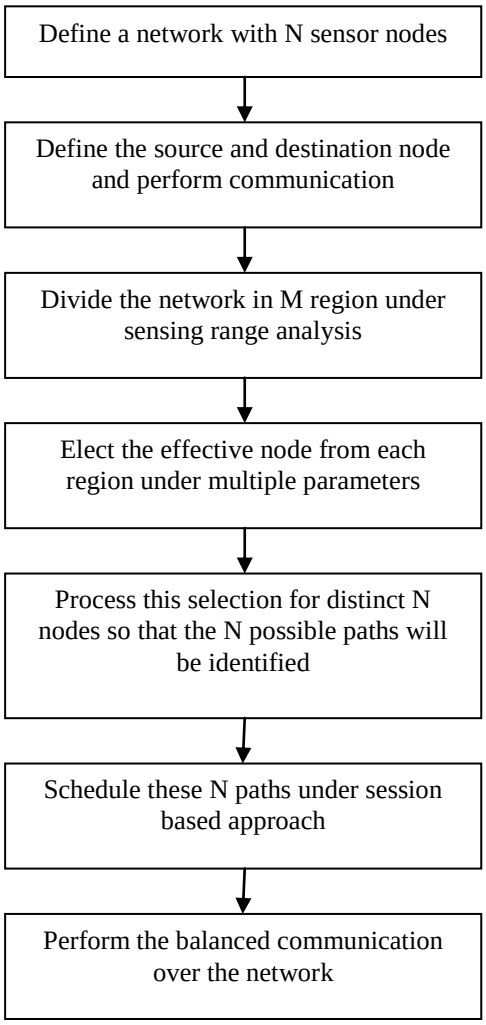

Figure 3: Adaptive Algorithmic Model

B) Layer II

Once the single path is obtained, the path nodes are excluded from the distance matrix and a new optimized path is generated over remaining network nodes. The path generation are here done under same communication and architectural node parameters. Based on these parameters, the distinctive paths are generated over the network nodes. The path nodes obtained from one path are node included in other path. In this work, M different paths are generated for network route optimization.

C) Layer III

In final stage of this work, the generated paths are applied sequentially. These paths are activated alternatively so that the load distributed communication will be performed. This distributed load mechanism has reduced the energy consumption on each path nodes so that the overall network life is improved.

IV. RESULTS

The presented work is simulated in MATLAB environment with random scenario. In this scenario, the nodes are placed randomly with random specification of energy. The communication constraints are also defined in terms of energy consumption associated with different communication operations. The communication is performed for 100 rounds and the analysis of work is done in terms of network energy and life parameters. The comparative analysis is done respective to 1-path routing and proposed M-path routing model. The comparative results obtained from the work are discussed in this section.

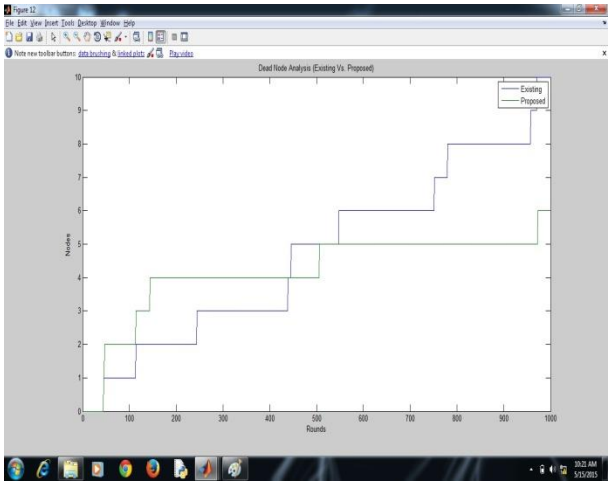

Figure 4: Dead Node Analysis

Here figure 4 is showing the comparative analysis of existing and proposed work under dead node analysis. The figure is showing the analysis in terms of dead nodes over the network. Here x axis is showing the communication rounds and y axis is showing the dead nodes. The figure shows that the dead nodes in case of existing approach are higher than proposed work. It shows that the overall network life in case of proposed work is improved. Another parameter considered relative to life is energy consumption in the network. The comparative analysis under this parameter is shown in figure 5.

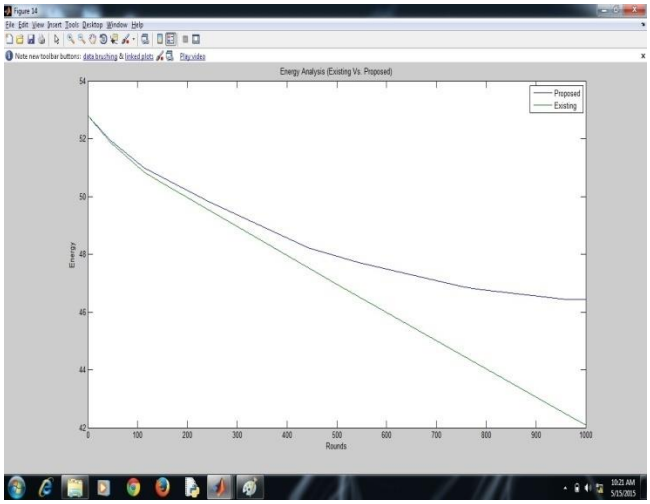

Figure 5: Network Energy Analysis

Here figure 5 is showing the comparative analysis in terms of network energy. The figure shows that the energy consumption in case of proposed work is much lesser then existing approach. It shows that the overall energy consumption in network is reduced and overall network life is improved.

V. CONCLUSION

In this paper, an adaptive M-Path based routing approach is defined to optimize the communication in sensor network. The presented work model is defined as the layered model in which the path load is reduced and the network life is improved. The results show that the work has improved the network life and reduced the energy consumption over the network.

REFERENCES

[1] Charlie Isaksson," Risk Leveling of Network Traffic Anomalies", IJCSNS International Journal of Computer Science and Network Security
[2] Li Yao," Anomaly Detection and Location with an Application to an Energy Management System".
[3] Peyman Kabiri," Research on Intrusion Detection and Response: A Survey", International Journal of Network Security
[4] RAHUL KHANNA, "Control Theoretic Approach To Intrusion Detection Using A Distributed Hidden Markov Model".
[5] Pengfan Yan," Detection of Suspicious Patterns in Secure Physical Environments".
[6] Kapil Kumar Gupta," Conditional Random Fields for Intrusion Detection".
[7] Jo˜ao B. D. Cabrera," Detection and Classification of Intrusions and Faults using Sequences of System Calls".
[8] Sandip Ashok Shivarkar," Hybrid Approach for Intrusion Detection Using Conditional Random Fields", International Journal of Computer Technology and Electronics Engineering (IJCTEE)
[9] Richard J. Bolton," Statistical Fraud Detection: A Review".
[10] Ramkumar Chinchani," RACOON: Rapidly Generating User Command Data For Anomaly Detection From Customizable Templates".
[11] Ping Yan," Anomaly Detection in theWIPER System Using Markov Modulated Poisson Process".
[12] K. Hanumantha Rao," Implementation of Anomaly Detection Technique Using Machine Learning Algorithms", International Journal of Computer Science and Telecommunications

