ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Novel Probability Model to Analyse Redundancy Management for Multipath Routing in Heterogenous Wireless Sensor Network

[I]Vinoshiya.G, [II]Krishnaveni.P, [III]Dr. J.Sutha
[I]PG Student, [II]Assistant Professor, [III]Professor and Head
[I,II,III]Dept. of CSE, Sethu Institute of Technology, Madurai, India

Abstract
In Intra-Cluster Scheduling and Inter-Cluster multi-hop routing schemes to maximize network processing time.A Heterogenous Wireless Sensor Network (HWSN) having larger energy and processing capabilities and failures are occurred to predict the malicious. In this project use a Multipath Routing, it is the routing technique of using multi alternative paths through the network, which can yield a variety of benefit such as fault tolerance, increased bandwidth and improved security. To develop a novel probability model to analyse the best redundancy level for path redundancy and source redundancy and provide the best intrusion detection. Intrusion Detection System (IDS) is a device or software that monitors network for malicious activities and produces reports to management station.

Keyword
Heterogenous Wireless Sensor Network (HWSN), Multipath Routing, Novel Probability Model , Intrusion Detection System (IDS), Fault Detection and Identification(FDI)

I. Introduction

A Wireless Sensor Network(WSN) consists of spatially distributed autonomous wireless sensor nodes. A node in a Wireless network is able to collect the information from sensors, process it and communicate wirelessly with other nodes in the network. It is used to monitor physical or environmental condition such as temperature, sound, vibration, pressure and pass their data through the network. A WSN is a self configuring network of small sensor nodes communicating among themselves using radio signals and deployed in quantity to sense monitor and understand the physical world. WSN are called motes. WSN has wide range of application to industry, science, transportation, civil infrastructure and security. Heterogenous Wireless Sensor Network (HWSN) consists of sensor nodes with different capacity, different computing power and different sensing range. Sensor node are battery powered device, hence it reduce the energy consumption

A. Components of WSN

A typical sensor network device comprises the following components some of which are optional:microcontroller, wireless communication channel, wired communication, sensor, power supply,local storage and real time clock systems. The principal idea is that the sensors are connected to a tiny computer that coordinates the measurement, preprocessors, stores and delivers the information.

1. Microcontrollers

Microcontrollers used in wireless low power,small profile,built in peripherals and on chip RAM and flash memory.

2. Radio Transceivers

Components used in a transceivers are low noise amplifer(LNA), mixer,variable gain amplifier(VGA), modulator,demodulator, filters, power amplifier(PA).

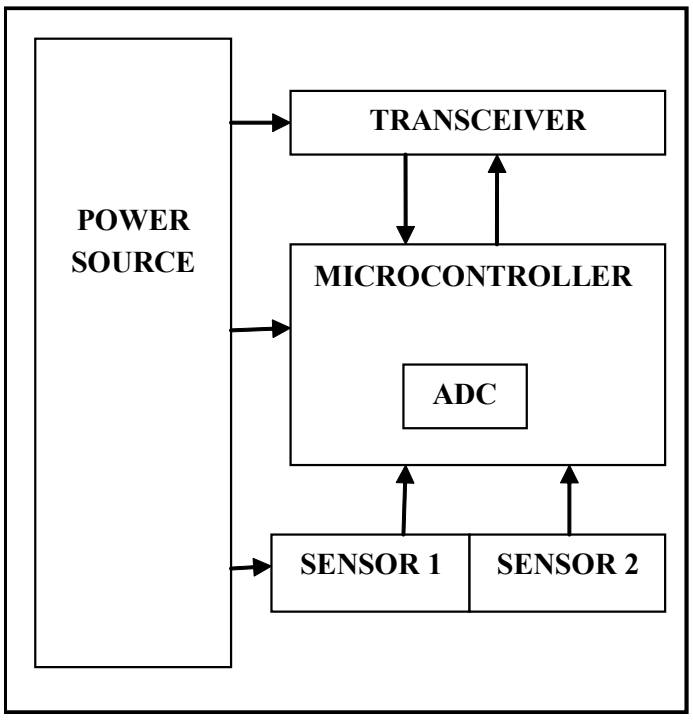


Figure 1: Block Diagram of WSN

3. Sensors

Sensors used in WSN may be onboard and external sensors, Various types of sensors like temperature sensors, voltage sensors, photo sensors, humidity sensors, vibration sensors are used.

4. Power /Batteries

Power option in sensor network may be battery operated, solar power and DC power.

B. Requirement and Design Factor in WSN

Following are some of the basic requirements and design factors of WSN which serves as guidelines for development of protocol.

1. Fault Tolerance
The network are used to detect failure of a node and organize itself, reconfigure and recover from node failures without losing any information.

2. Power Management
The Wireless sensor node contain a microelectronic device, equipped with a limited power source.Solar energy is used for empowering remote sensor node exposed for environment.

3. Energy Efficiency
Sensor node have a small and finite source of energy. Both hardware ad software related is proposed to optimize energy use.

4. Routing
Routing algorithms are used to find minimum hop and shortest distance paths for transfer the data.

5. Management Challange
Managing the communication over heterogeneous network is the basic challenge in self-managed system because policies and communication protocols plan an important role in network communication.

6. Life Time
The Primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize network lifetime.

C. Application
Area Monitoring is the common application of WSN. It is used to deployed over a region where some phenomenon is to be monitored. Environmental Sensing is used to cover the earth science research, includes sensing volcanoes, oceans, glaciers, forests. Industrial monitoring is used in machine health monitoring, water/waste monitoring in industries, agriculture and structural monitoring.

II. Literature Review
Machado et al., Suggested [16] the design of heterogenous two-tier WSN, where one tier of nodes is more robust and computationally intensive than the other tier. To find the ratios of densities of nodes in each tier to maximize coverage and network lifetime.

Chen et al., Suggested [18] the data sensing are used in wide spread application in area such as securiry and surveillance monitoring and command, control in battle field. To develop adaptive fault-tolerant quality of service (QOS) control algorithm based on hop-by-hop data delivery utilizing source and path redundancy, with the goal to satisfy application QOS requirements.

Bao et al.,Suggested [19] the scalable cluster-based hierarchical trust management protocol for WSN to effectively deal with malicious nodes.. A novel probability model describe a HWSN comprising a large number of sensor nodes with different social and quality of service (QOS) behaviours. Anomaly based intrusion detection used in both the detection probability and false positive probability

Ren Fengyuan et al., Suggested [20] the sensor nodes have more redundancy, data aggregation becomes an effective method to eliminate redundancy, minimize the number of transmission and then to save energy. The attribute-aware data aggregation provide parameters, such as scalable with respect to network size and adaptable for tracking mobile events.

III. Existing System
In existing sytem, the heterogenous wireless sensor network of dynamic redundancy management of multipath routing is used[16]. In this algorithm, the data in each node can be changed dynamically and does not find the malicious node easily. The multisource multipath data routing transfer the data in the presence of unreliable and malicious node. It leads to speed for the data transfer is low,the processing time is high and more energy is required.

IV. Proposed Algorithm
Intrusion Detection System (IDS) [10] is a device or software application that monitors network or system activities for malicious activities and produces reports to a management station. Intrusion Detection and prevention System (IDPS) are primarily focused on identifying possible incidents, logging information about them and reporting attempts.

A. Network Formation
The Network Formation is the process of creating the node. The node are allocated in separated manner. It is used to define the size and structure of each node.

B. Neighbor Discovery
Neighbor Discovery [15] is used to perform route discovery. Each node that find the available router and link of the address. It determine the path of the neighbor node.

C. Checking Cluster
Each node is verified by the cluster head. It completed its verification and it then send the request.

D. Send Request
The request is given from source to destination node. The node checks whether the request is given or not from source to destination. If the node has any fault,the output is given to the IDS.

E. IDS
IDS [10] monitors the system, identifies the interference or collided node while transferring the data and information present in each node should be checked. Avoid the traffic ,fault each node, identifies the collision occurred in each node and transfers the node in efficient manner.

F. Performance Evaluation
It is easy to find the malicious node,avoids traffic signal and reduce the delay during data transfer.And finally transfer the data in efficient manner.

1. Packet Received

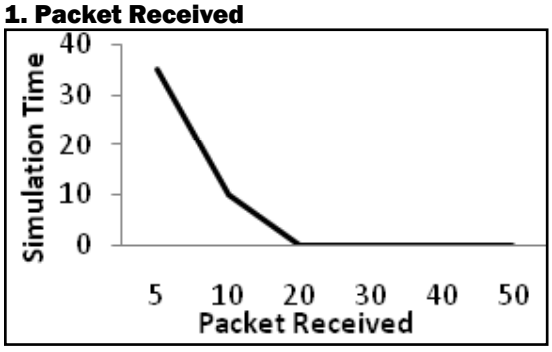


Figure 2 Packet Received

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

In Figure 2, every node is verified by the cluster head, if it contain any fault it use the IDS algorithm to remove the fault node and send the node to destination.

2. Active Node

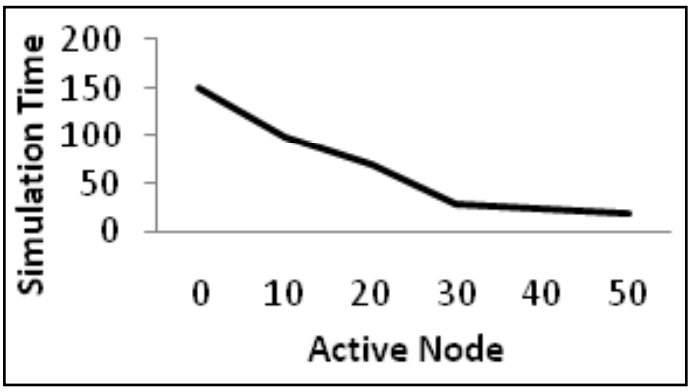
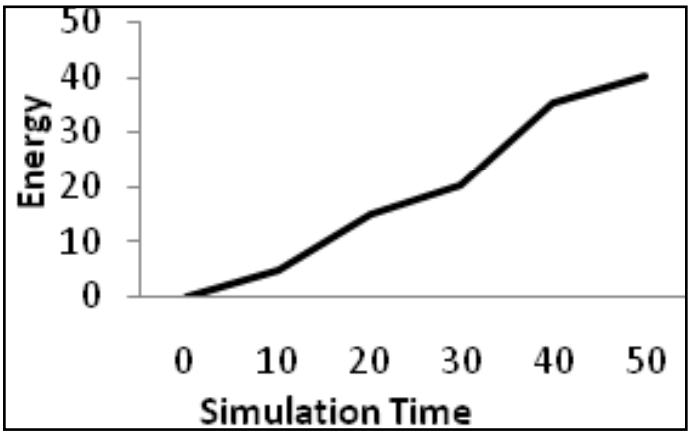


Figure 3 Active Node

In Figure 3, the graph represent the number of active node activated at a certain amount of simulation time.When the active node is increased the simulation time also gets increased.

3. Energy Consumption



The Figure 4 Energy Consumption

In Figure 4, it describe the relationship between the simulation time and energy . The energy is depend upon the simulation time. If the time increases, the energy also increase.

V. Conclusion

A HWSN is maximized for reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. The design of a dynamic redundancy management algotithm to identify and apply the best design parameter settings at runtime in response to prolong the system lifetime. HWSN utilize multipath routing, used to minimize the energy consumption and reduce the failure node and transfer the information in security manner.

VI. Future Enhancement

In Future enhancement, Fault Detection and Identification (FDI) algorithm management is applied to detect malicious nodes in a wireless network. FDI is the subfield of control engineering which itself monitoring a system, identifying when a fault has occurred and pointing the type of fault and its location. Direct pattern recognition of sensor reading that indicate a fault and an analysis of the discrepancy between the sensor readings and expected values. And it can reduce the error.

References

[1] *S. T. Cheng, C. M. Chen and I. R. Chen, "Dynamic quata-based admission control with subrating in multimedia servers," 2000.*

[2] *W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans.Wireless commun., 2002.*

[3] *S. T. Cheng, C. M Chen and I.R. Chen, "Performance evaluation of an admission control algorithm:dynamic threshold with negotiation," 2003.*

[4] *S. Zhu, S. Setia and S. Jajodia, "LEAP: efficient security mechanisms for large –scale distributed sensor networks," 2003.*

[5] *S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks ," 2003.*

[6] *O. Younis and S. Fahmy, "HEED:a hybrid,energy-efficient,distributed clustering approach for ad-hoc sensor networks," 2004.*

[7] *M.Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. LIU and S.Singh, "Exploiting heterogeneity in sensor networks," 2005.*

[8] *A. P. R Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," 2005.*

[9] *E. Felemban, L. Chang-Gun and E. Ekici, "MMSPEED: Mutipath Multi-Speed protocol for QOS guarantee of reliability and timeliness in wireless sensor networks," 2006.*

[10] *J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," 2006.*

[11] *I. Krontiris, T. Dimitriou and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 2007.*

[12] *H. Su and X. Zhang, "Network lifetime optimization for heterogenous sensor networks with mixed communication modes,"2007.*

[13] *H. M. Ammari and S. K. Das, "Prmoting heterogeneity, mobility and energy-aware voronoi diagram in wireless sensor networks," 2008.*

[14] *S. Rajasegaran, C. Leckie and M. Palaniswami, "Anomaly detection in wireless sensor networks," 2008.*

[15] *Y. Lan, L. Lei and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection ," 2009.*

[16] *R. Machado, N. Ansari, G. Wang and S. Tekinay, "Adaptive density control in heterogenous wireless sensor networks with and without power management," 2010.*

[17] *T. Shu, M. Krunz and S. Liu, " Secure data collection in wireless sensor networks using randomized dispersive routers ," 2010.*

[18] *I. R. Chen, A. P. Speer and M.Eltoweissy, " Adaptive Fault-Tolerant QOS control algorithms for maximizing system lifetime of query-based wireless sensor networks," 2011.*

[19] *F. Bao, I. R. Chen, M. Chang and J. Cho, "Hierarchical trust management for wireless sensor network and its applications to trust based routing and intrusion detection," 2012.*

[20] *Ren Fengyuan, Zhang, Jiao Wu, Yongwei, and He Tao, " Attribute-aware data aggregation using potential based*

dynamic routing in wireless sensor networks ," 2013.

G.Vinoshiya received her B.Tech., degree in Information Technology from Anna University at Syed Ammal Engineering College,Ramanathapuram in 2012.She is currently pursuing her M.E.,degree in Computer and Communication Engineering from Anna University at Sethu Institute of Technology,Virudhunagar.