Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-7, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Data Center Network

R. Yogeswaran[1] & E. Vanitha[2]
[1]PG Scholar, Department of CSE, PTR Engineering college, Madurai, India
[2]Assistant Professor, Department of CSE, PTR Engineering College, Madurai, India

Abstract: *Redundancy Management is a technique in which a user would issue a query and expect a response to be returned within the deadline. While the use of fault tolerance mechanisms through redundancy improves query reliability. It can develop a mathematical model for the lifetime of the sensor system as a function of system parameters including the "source" and "path" redundancy levels utilized. Data sensing and retrieval in wireless sensor systems have a widespread application in areas such as security and surveillance monitoring. Redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. Which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability. It applied related analysis results to the design of a dynamic redundancy management. The best design parameter settings at runtime in response to environment changes to prolong the system lifetime.*

1. Introduction

Wireless sensor network (WSN) is a key element of the pervasive/ubiquitous computing. With the advancement of manufacturing and wireless technologies, many feasible applications are proposed such as industrial sensor networks, volcano-monitoring networks, and habitat monitoring etc. The heterogeneous WSN consists of sensor nodes with different abilities, such as various sensor types and communication/sensing range, thus provides more flexibility in deployment. For example, it can construct a WSN in which nodes are equipped with different kinds of sensors to provide various sensing services.

Besides, if there are two types of senor nodes: the high-end ones have higher process throughput and longer communication/sensing range; the low-end ones are much cheaper and with limited computation and communication/sensing abilities. A mixed deployment of these nodes can achieve a balance of performance and cost of WSN. For example, some low-end sensor nodes can be used to replace high-end ones without degrading the network lifetime of WSN.

Many research works have been proposed to address the deployment problem of heterogeneous WSN. To achieve a satisfying performance, the deployment of heterogeneous WSN is more complicated than homogeneous WSN. To maintain a symmetric communication, the distance between high-end and low-end sensor nodes cannot be larger than the maximum communication range of the low end one. Besides, if the sensor nodes have different detection range, the sensor coverage area of low-end node cannot be fully covered by the high-end node.

Recent advances in wireless communication technologies and the manufacture of inexpensive wireless devices have led to the introduction of low-power wireless sensor networks. Due to their ease of deployment and the multi-functionality of the sensor nodes, wireless sensor networks have been utilized for a variety of applications such as healthcare, target tracking, and environment monitoring. The main responsibility of the sensor nodes in each application is to sense the target area and transmit their collected information to the sink node for further operations. Resource limitations of the sensor nodes and unreliability of low-power wireless links, in combination with various performance demands of different applications impose many challenges in designing efficient communication protocols for wireless sensor networks. Meanwhile, designing suitable routing protocols to fulfill different performance demands of various applications is considered as an important issue in wireless sensor networking.

In this context, researchers have proposed numerous routing protocols to improve performance demands of different applications through the network layer of wireless sensor networks protocol stack. Most of the existing routing protocols in wireless sensor networks are designed based on the single-path routing strategy without considering the effects of various traffic load intensities. In this approach, each source node selects a single path which can satisfy performance

requirements of the intended application for transmitting its traffic towards the sink node. Although route discovery through single-path routing approach can be performed with minimum computational complexity and resource utilization, the limited capacity of a single path highly reduces the achievable network throughput.

Furthermore, the low flexibility of this approach against node or link failures may significantly reduce the network performance in critical situations. For instance, whenever the active path fails to transmit data packets (as a result of limited power supply of the sensor nodes, high dynamics of wireless links and physical damages), finding an alternative path to continue data transmission process may cause extra overhead and delay in data delivery. Therefore, due to the resource constraints of sensor nodes and the unreliability of wireless links, single-path routing approaches cannot be considered effective techniques to meet the performance demands of various applications. In order to cope with the limitations of single-path routing techniques, another type of routing strategy, which is called the multipath routing approach has become as a promising technique in wireless sensor and ad hoc networks. Dense deployment of the sensor nodes enables a multipath routing approach to construct several paths from individual sensor nodes towards the destination. Discovered paths can be utilized concurrently to provide adequate network resources in intensive traffic conditions. Alternatively, each source node can use only one path for data transmission and switch to another path upon node or link failures.

The latter one is mainly used for fault-tolerance purposes, and this is known as alternative path routing. In the past decade, multipath routing approach has been widely utilized for different network management purposes such as improving data transmission reliability, providing fault-tolerant routing, congestion control and Quality of Service (QoS) support in traditional wired and wireless networks. However, the unique features of wireless sensor networks (e.g., constrained power supply, limited computational capability, and low-memory capacity) and the characteristics of short-range radio communications (e.g., fading and interference introduce new challenges that should be addressed in the design of multipath routing protocols.

Accordingly, existing multipath routing protocols proposed for traditional wireless networks (such as ad hoc networks) cannot be used directly in low-power sensor networks. During the past years, this issue has motivated the research community of wireless sensor networks to develop multipath routing protocols which are suitable for sensor networks.

2. Related Works

Optimal parameters for the algorithm

The Sensors in the wireless sensor network are distributed as per a homogeneous spatial Poisson process. All Sensors transmit at the same power level and hence have the same radio range. Data exchanged between two communication sensors not within each others. Each sensor uses 1 unit of energy to transmit or receive 1 unit of data.

LPD algorithm

In order to perform multi path data transmission. A low reputation value for this environment which indicates there may be possible compromised nodes in the neighborhood. These metrics do not consider the security aspects of the path.

RSSI technique

After deployment when nodes perform neighbor discovery. The packet received with RSSI value that is not in the range cab be flagged. We focus only on intrusion detection and hence do not discuss solutions to handle intrusions. Received signal strength is related to the distance between nodes.

Trust-based geographic routing

A node disseminates a message to a maximum of neighbor closest to destination node. A node floods a message to all its neighbors+10. Until a copy of the packet reaches the destination nodes. It yields the highest message delivery ratio and lowest message delay at the expense of the highest message overhead. The average delay for those messages that are successfully delivered under various routing protocols.

3. Proposed Methodology

In the proposed methodology, the tradeoff between energy consumption and QoS gain particularly in reliability. In a randomized dispersive multipath routing protocol is proposed to avoid black holes. A decentralized rule based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The intrusion detection where the decision is based on a majority voting of monitoring nodes. Proposed for wired networks impractical for use in large-scale sensor networks. Every node shares a unique key with the base station. a reputation-based framework for data integrity in WSNs. scheme for WSN security, particularly for secure routing, where each node only maintains highly abstracted a hybrid trust and reputation management protocol for WSNs by combining certificate-based and behavior-based trust evaluations. Trust management scheme for clustered

WSNs in which each SN performs peer evaluation based on direct observations or recommendations.

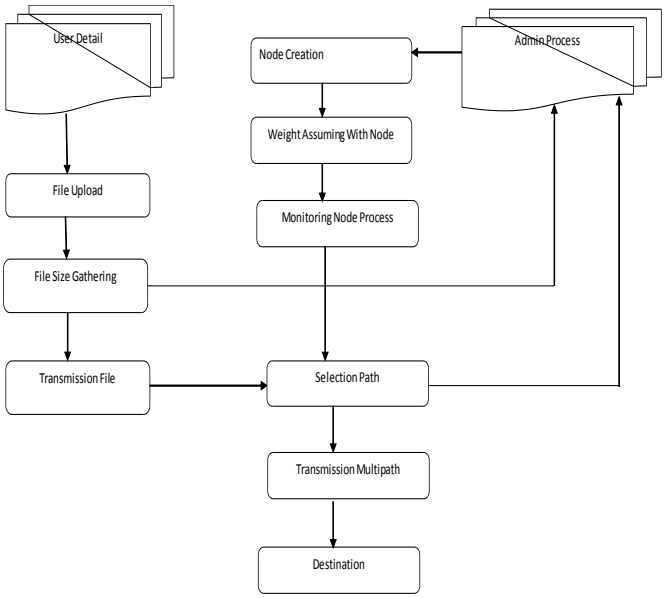

Fig. 1 Proposed method

Multipath Routing Algorithm:

Dynamic redundancy management is to dynamically identify and apply the best redundancy level in terms of path redundancy multipath routing is distributed in nature managing multipath routing for intrusion tolerance to maximize the system lifetime. They specify control actions taken by individual SNs and CHs in response to dynamically changing environments.

Multipath Routing Algorithm used any traffic occur user selection path that path was redirect into another path, so which path packet it should be send that node was sensing to adjust the optimal parameter setting in response to changing environments. Event is to adjust its radio range to maintain SN connectivity within a cluster. it triggers multipath routing for intrusion tolerance using the current optimal ms and mp settings to prolong the system useful lifetime.

Clustering Algorithm

The prescribed multipath routing protocol to route the packet. Each node periodically performs clustering as prescribed by the cluster algorithm timer event occurs; each node executes clustering for periodic cluster formation. Query processing through multipath routing, in terms of energy consumption has been considered. Eliminated if the CH notifies the optimal settings to its SNs at the time periodic clustering is performed

4. Experimental results

In these experimental results, can able to secure the sample data from the sender by using dynamic redundancy management algorithm energy saving path for transmission data. The below figures shows the proposed method result.

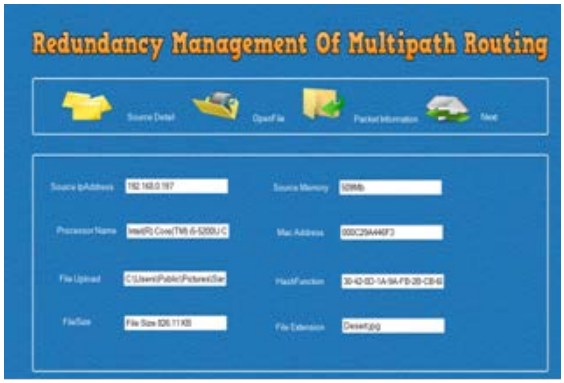

Fig.1 Source File details

Fig.2 Selecting Path

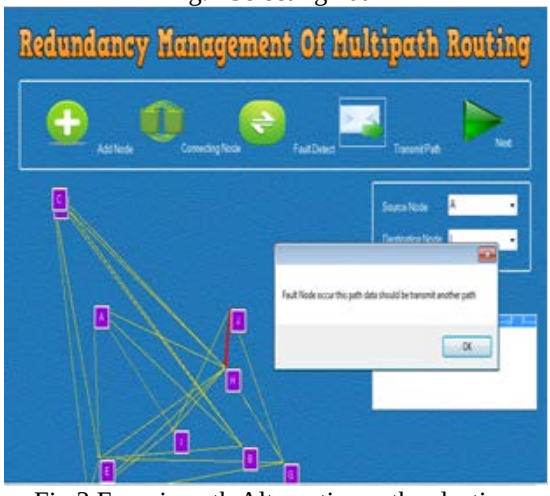

Fig 3 Error in path Alternative path selection

Fig.4 Energy saving path

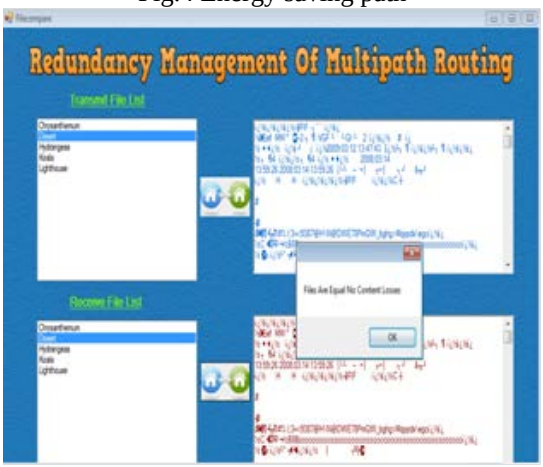

Fig.5 File Received and Acknowledged

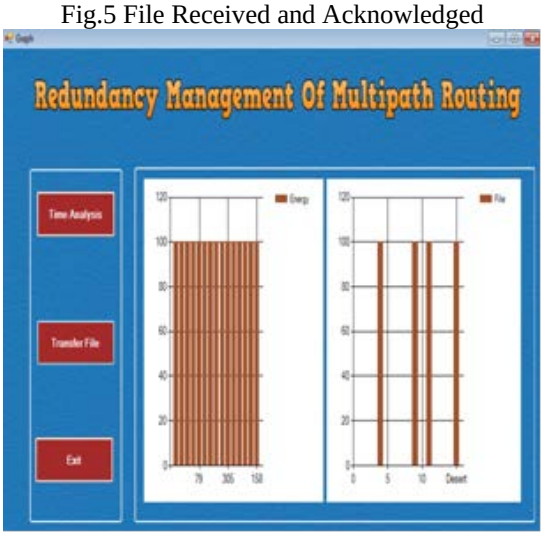

Fig. 6 Time Analysis and Transferred File

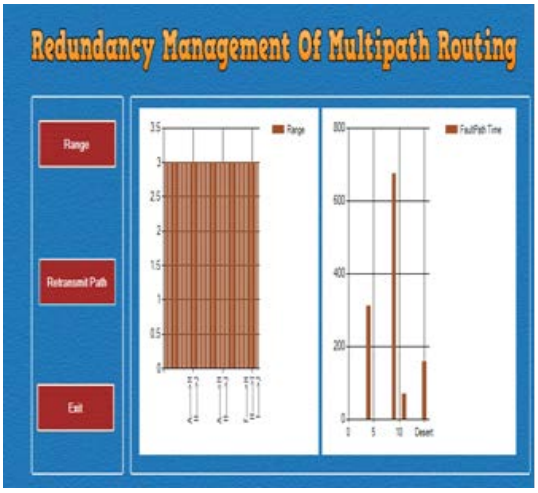

Fig. 7 Range and Retransmit path

In this process, based on redundancy management algorithm can find the energy saving path and transfer the file. And from the receiver an acknowledgment is received with "No DATA Loss".

7. CONCLUSION

In this paper, the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. Finally, applied our analysis results to the design of a dynamic redundancy management algorithm to identify as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. In situations where concurrent query traffic is heavy, thus plan to explore trust-based admission control.

REFERENCES

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," IEEE Trans. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.

II. M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890.

III. H. M. Ammari and S. K. Das, "Promoting heterogeneity, mobility, and energy-aware Voronoi diagram in wireless

sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995–1008, 2008.

IV. X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh. Technol. Conf., pp. 2528–2532.

V. S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007

VI. J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

VII. A. P. R. da 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," in Proc. 2005 ACM Workshop Quality Service Security Wireless Mobile Networking.