IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Multipath Routing Redundancy Management For Intrusion Tolerance In Heterogeneous Wireless Sensor Networks

SHIVANAND

Lecture Senior Scale, Department of Computer Science and Engineering
Government Polytechnic,Karatagi, Koppal,Karnataka, India

Abstract: In order to extend the useful life of a Wireless Sensor Network (WSN), Redundancy Management of Multipath Routing abstractions emphasize the use of many data pathways to improve system security and reliability against malevolent or unreliable nodes while balancing this against energy cost. In order to increase query success probability and network lifespan, these abstracts suggest voting-based intrusion detection techniques to find and eliminate malicious nodes, dynamic algorithms that modify settings at runtime in response to environmental changes, and mathematical models to determine the ideal redundancy levels for multipath routing.

Index Terms – Wireless sensor, Redundancy.

I INTRODUCTION:

Applications that report detected events of interest, like military surveillance and forest fire monitoring, are best suited for wireless sensor networks. Sensor nodes in wireless sensor networks are battery-operated and have very little computing power. A sensor node uses a multi-hop method to wirelessly transmit messages to a base station with a limited radio communication range. However, malicious attacks frequently target Wireless Sensor Networks' multi-hop routing. An attacker can physically alter nodes, cause traffic collisions with transmissions that appear legitimate, drop or reroute messages in routes, or use radio interference to jam the communication channel.

Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in have been proposed. The optimal communication range and communication mode were derived to maximize the Heterogeneous Wireless Sensor Networks lifetime. The authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchical with Cluster Head nodes having larger energy and processing capabilities than normal SNs. The solution is formulated a Heterogeneous Wireless Sensor Networks an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes. The authors considered a two-tier Heterogeneous Wireless Sensor Networks with the objective of maximizing network lifetime while fulfilling

power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime.

In wireless sensor networks, multipath routing is seen to be a useful technique for fault and intrusion tolerance that enhances data transmission. The basic premise is that the more pathways we have undertaking data transmission, the more likely it is that at least one path will reach the base station or sink node. Some consideration has been given to using multipath routing to withstand insider attacks, however the majority of earlier research was on using multipath routing to increase dependability. However, the trade-off between QoS improvement and energy consumption, which might negatively decrease the system lifetime, was generally overlooked in these research.

Objectives of the work:

This project's goal is to provide efficient data transmission in wireless sensor networks by implementing "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks."

II.LITERATURE REVIEW:

MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and Timeliness in wireless sensor networks

Multipath routing approach is used in wireless sensor networks to improve network performance through efficient utilization of available network resources. In Wireless sensor networks (WSNs) many multipath routing protocols have been designed to satisfy the QoS requirements such as reliability, security, delay, timeliness and to improve the network lifetime. Multipath routing is an efficient technique, which selects multiple paths to deliver data to the base station. This analyses the performance of various multipath routing protocols such as ReIn For MH-SPREAD, MMSPEED, and MCMP, ECMP which are designed to provide reliable data transmission.

Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks

Data sensing and retrieval in wireless sensor systems have a widespread application in areas such as security and surveillance monitoring, and command and control in battlefields. In query-based wireless sensor systems, 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 in the presence of unreliable wireless communication and sensor faults, it could cause the energy of the system to be quickly depleted. Therefore, there is an inherent trade-off between query reliability versus energy consumption in query-based wireless sensor systems. In this paper, we develop adaptive fault-tolerant quality of service (QoS) control algorithms based on hop-by-hop data delivery utilizing "source" and "path" redundancy, with the goal to satisfy application QoS requirements while prolonging the lifetime of the sensor system. We 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. We discover that there exists optimal "source" and "path" redundancy under which the lifetime of the system is maximized while satisfying application QoS requirements. Numerical data are presented and
validated through extensive simulation, with physical interpretations given, to demonstrate the feasibility of our algorithm design.

Improving routing in sensor networks with heterogeneous sensor nodes

One of the most important applications of the wireless sensor networks is the widely applied smart environment. To prolong the network lifetime, it is important to develop the protocols for reducing energy consumption because the sensor nodes are constrained by limited energy. In the cluster based on energy-

efficient method, the fixed cluster head number, the energy of the node, and the transmission distance are the keys to extending the network lifetime. In this paper, we propose an improved grouping protocol, which considers the distance between the sensor node and the sink node in order to allocate total energy of a group. The proposed method is compared with previous works of simulations to show the advantages of extending the network lifetime.

III.PROBLEM DEFINATION:

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The trade off between energy consumption vs. reliability gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the trade off in the presence of malicious attackers.

It is commonly believed in the research community that clustering is an effective solution for achieving scalability, energy, conservation and reliability. Using homogeneous nodes which rotate among themselves in the roles of and sensor nodes (SNs) leveraging election protocols such as HEED for lifetime maximization has been considered. Recent studies demonstrated that using heterogeneous nodes can further enhance performance and prolong the system lifetime. In the latter case, nodes with superior resources serve as performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. The trade off issue between energy consumption vs. QoSgain becomes much more complicated when inside attackers are present as a path may be broken when a malicious node is on the path.This is especially the case in heterogeneous WSN (HWSN) environments in which nodes may take a more critical role in gathering and routing sensing data. Thus, very likely the system would employ an intrusion detection system(IDS) with the goal to detect and remove malicious nodes.

System Requirements and Specifications:

The behaviour of the system that has to be constructed is fully described in a Software Requirements Specification (SRS). The software product's functional requirements can be found by applying the use case technique. Non-functional (or supplemental) needs are also included in SRS. Requirements that provide limitations on the design or implementation are known as non-functional requirements. Examples of these include design restrictions, performance engineering requirements, and quality standards. There are two fundamental tasks in the SRS phase. (1) Analysis of Problems and Requirements (2) Overview of Product Function

Functional Requirements

Our developed system must perform the required functions.

- It has to find routing table from source to destination on demand as and when necessary as it changes the topology.
- Our proposed system should find not a single shortest path it has to finds all available multiple path from source to destination.
- Out proposed system should broadcast the message to destination through all available multiple path for reliability of data transmission.
- Prepare IDS system to detect redundancy path which is present multiple path to avoid traffic and collision of data during data transmission by which throughput is increases.
- Send data from those path which is eliminated from redundancy.

Hardware and Software Requirements

- **Hardware Requirements**

- PROCESSOR : PENTIUM IV 2.6 GHZ
- RAM : 512 MB DD RAM
- HARD DISK : 20 GB
- KEYBOARD : STANDARD 102 KEYS

- **Software Requirements**

- FRONT END : JAVA, J2EE
- DATA BASE USED : My-SQL
- TOOLS USED : NET BEANS IDE6.9.X (OPTIONAL)
- OPERATING SYSTEM : WINDOWSXP

Architecture Diagram

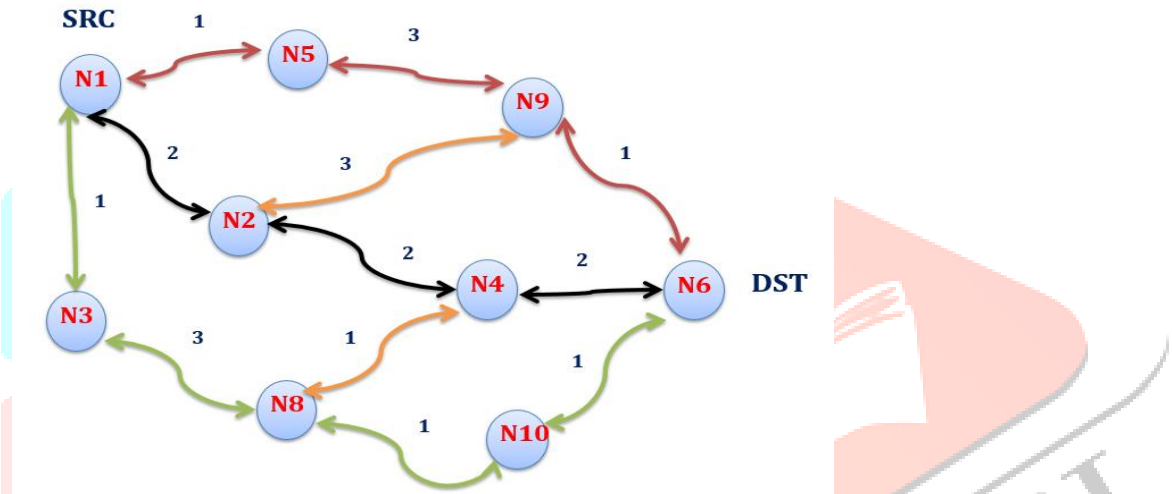

Fig.1:Source and path redundancy for heterogeneous wireless sensor network

Activity Diagram

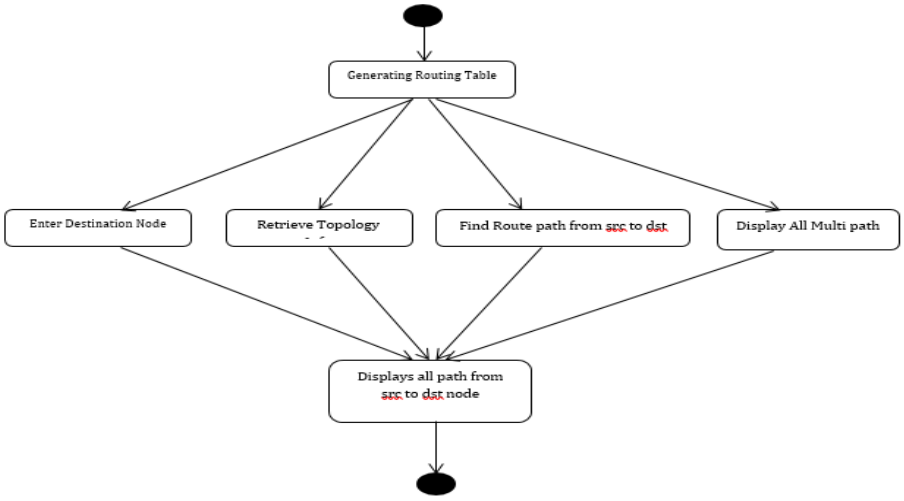

Fig.2:Activity Diagram for Source Node Route finding

IV. RESULT AND DISCUSSION:

MODULES

1. Multi – Path Routing
2. Intrusion Tolerance
3. Energy Efficient

Modules Description

1. **Multi – Path Routing**

In this module, Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of atleast one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

2. **Intrusion Tolerance**

In this modules, intrusion tolerance through multipath routing, there are two major Problems to be solved:

(1) How many paths to use and

(2) What paths to use.

To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols.

3. **Energy Efficient**

In this module, there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbour nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host-based IDS for energy conservation.

Class diagrams for sender, receiver and neighbouring node :

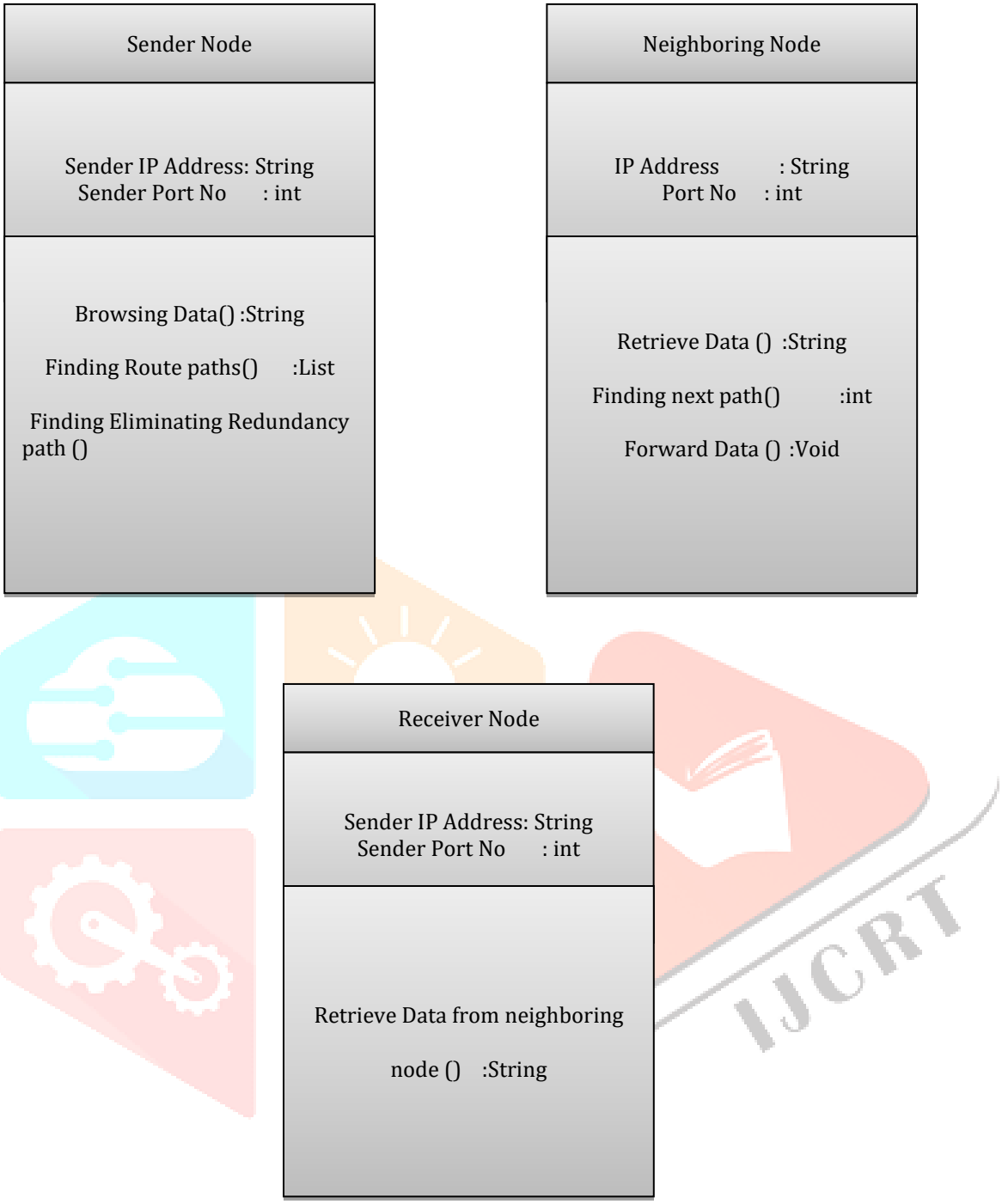

Fig. 3:class diagrams for sender, receiver and neighbouring node

Sequence Diagram of load balancing in multipath flow-slice

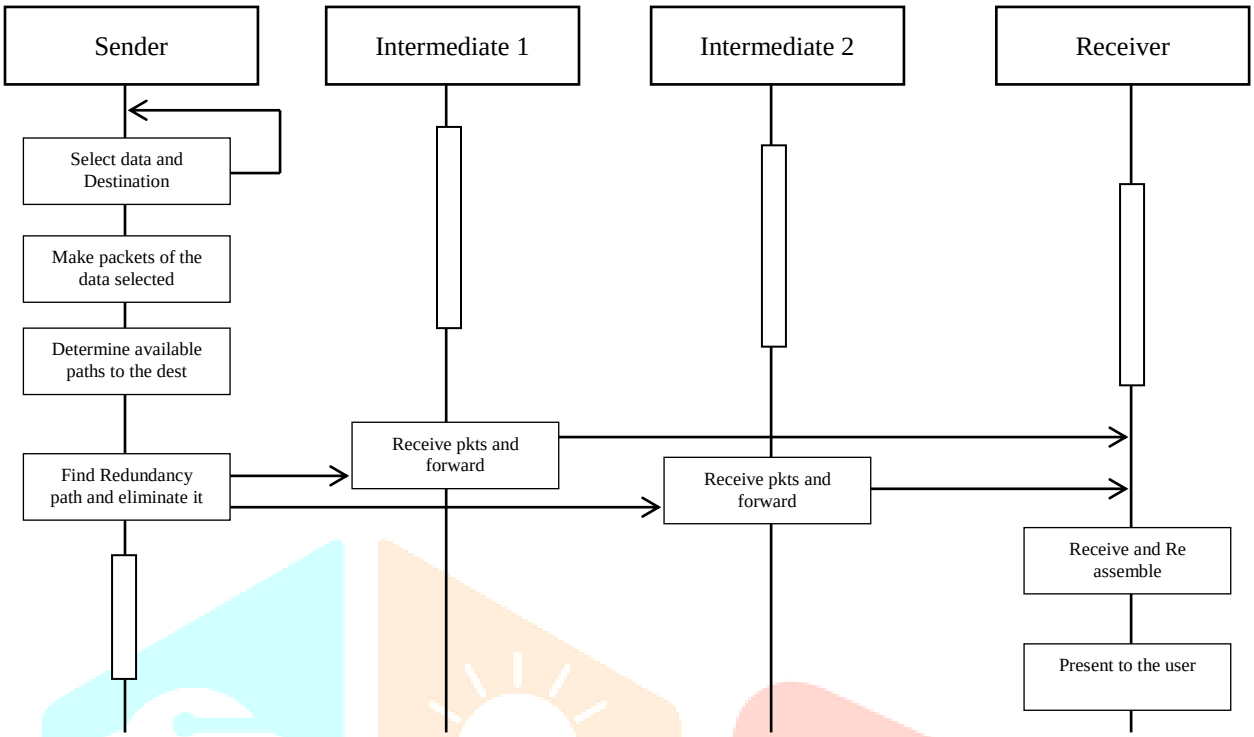

Fig.4: Sequence diagram for load balancing in multipath flow-slice

V.CONCLUSION:

In order to manage redundancy in clustered heterogeneous wireless sensor networks, we conducted a tradeoff analysis between energy consumption and QoS gains in timeliness and dependability.To determine the optimal redundancy level in terms of source redundancy (ms) and path redundancy (mp), we are creating a novel probability model.

REFERENCE:

[1] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Computing., vol. 3, no. 4, pp. 366-379, 2004.
[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks," IEEE Trans. Mobile Computing., vol. 5, no. 6, pp.738-754, 2006.
[3] 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. on Dependable and Secure Computing, vol. 8, no. 2, pp. 161-176, 2011.
[4] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," 24th Annu. Joint Confof the IEEE Computer and Communications Societies (INFOCOM),2005, pp. 878-890 vol. 2.