**MAXIMIZING THE LIFETIME OF HETEROGENEOUS WIRELESS SENSOR NETWORKS USING MULTIPATH ROUTING TECHNIQUE**

SHAIK ANSAR BASHA, CH. SUBBARAO, P.BABU

1Pg Scholar, CSE,Quba Engineering College,Nellore
2Associate Professor,CSE,Quba Engineering College,Nellore
3Associate Professor,CSE,Quba Engineering College,Nellore

**ABSTRACT:** Heterogeneous Wireless sensor network (HWSN) is group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment. Heterogeneous Wireless Sensor Networks (HWSNs) are used for various applications such as habitat monitoring, automation, agriculture, and security. Wireless sensor network consists of large number of small nodes. The nodes then sense environmental changes and report them to other nodes over flexible network architecture. Heterogeneous WSNs are deployed in an unattended environment in which energy replenishment is very difficult. Due to limited resources, a Heterogeneous WSN must not only satisfy the application specific Quality of service (QoS) requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff issue between energy consumption vs. QoS gain becomes much more complicated when inside attackers or intruders are present in the network, as a path may be broken when a malicious node is on the path. The main goal of this paper is to exploit the tradeoff between energy consumption vs. the gain in reliability and security to maximize the system useful lifetime in the presence of attackers. The clustering of nodes is performed to increase the performance and decrease the energy consumption at each node. The energy efficiency is achieved by restricting the communication between inter cluster sensors which are far apart from each other and also by introducing a distributed intrusion detection system to detect and evict the malicious nodes causing certain types of energy consuming attacks.

To satisfy the reliability requirement of a Heterogeneous WSN, a modified multipath routing scheme is proposed. The optimal amount of redundancy that has to be applied to achieve reliable yet energy efficient data transfer will be estimated. Thus the proposed methodology satisfies both the energy efficiency and reliability requirements of a WSN in the presence of malicious nodes.

**KEY WORDS:** Heterogeneous wireless sensor networks, multipath routing, intrusion detection, reliability, security, energy conservation.

**I. INTRODUCTION**

Wireless sensor networks (WSN) is a growing technology which is offering solution for many Application areas such as health care, military, industry and also environmental conditions like temperature, sound, gas, pressure. SNs are used for sensing the environments are used to read the sensing information and transmit to base station and also used for monitoring purposes. Sensor node is a tiny device includes five basic components 1)controller 2)communication devices 3)sensors/actuators 4) memory 5) power supply. These sensor networks are used for many critical applications where security is also critical and energy replacement is difficult if not impossible. So it is important satisfy application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to extend the system useful period of time. The trade of between energy consumption and gain in reliability gain with goal maximize the WSN system lifetime has been well explored in the literature. However, no prior work exits to consider the trade-off within the presence of malicious attackers. Naturally, grouping of sensor nodes in to clusters has been widely used in research community to satisfy scalability and generally achieve high energy efficiency and prolong the network lifetime in large-scale WSN environment. In the hierarchical network structure each cluster has a leader which also called as cluster head (CH) and usually performs the special tasks referred above (fusion and aggregation), and several common sensor nodes (SN) as members. The cluster formation process eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes periodically transmit their data to the corresponding CH nodes. On the other hand, security in WSNs is an important issue, especially if they have mission-critical tasks. For instance, a confidential patient health record should not be released to third parties in a health care application. Securing WSNs is critically important in tactical (military) applications where a security gap in the network would cause causalities of the friendly forces in a battlefield. Security attacks against WSNs are categorized into two main branches: Active and Passive. In passive attacks, attackers are typically camouflaged (hidden) and either tap the communication link to collect data; or destroy the functioning elements of the network. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering/ destruction and traffic analysis types. In active attacks, an adversary actually affects the operations in the attacked network. This effect may be the objective of the attack and can be detected. For example, the networking services may be degraded or...
terminated as a result of these attacks. Active attacks can be grouped into Denial-of-Service, black hole, wormhole, sinkhole, etc.), flooding and Sybil types. The basic idea is that heterogeneous wireless sensor network (HWSNs) nodes having wireless link with dissimilar communication range, sensing range, densities and capabilities. It increases the network lifetime and reliability and energy also achieved. Intrusion detection system (IDS) is used to detect malicious nodes. Two problems will arise:1) what paths to use and 2) how many paths to use and to overcome this problem multipath routing is used, is a routing technique of using multiple alternative paths through a network.

1.1 OBJECTIVE OF PAPER

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. 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 at least 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 trade-off between QoS gain vs. energy consumption which can adversely shorten the system lifetime. The research problem we are addressing in this paper is effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. We address the trade-off between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime.

1.2 PROBLEM DEFINITION

The packet will be dropped by head of the cluster, when the data has been already sent. If the packet has not been dropped then the cluster head or the node which did not drop the packet behaves as a malicious node. The function of no dropping the packet is Bad Mouthing. This is a main problem when in the redundancy, wireless sensor networks. When some nodes in a cluster group need to send some data to other cluster node. The nodes which need to send information will approach the cluster head of the then the data has been sent to head of the cluster. Each and every cluster will have direct connection or an indirect connection to process through the cluster head. Now, head of the cluster will get the data and send the data to the head processor.

II. LITERATURE SURVEY

2.1 INTRODUCTION

A literature survey or literature review means study of references papers and old algorithms that we have read for designing the proposed methods. It also helps in reporting summarization of all the old references papers, their drawbacks. The detailed literature survey for the project helps in comparing and contrasting various methods, algorithms in various ways that have implemented in the research. The literature study prescribed in this research of the project supports high availability of data, various algorithms, various old references papers, comparison of the methods. This design supports various types of attacks preventions like combined cryptography methods, strong commitment methods, elliptic method and all or nothing methods.

2.2 RELATED WORK

- Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed.
- In the optimal communication range and communication mode were derived to maximize the HWSN lifetime.
- In devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs.
- The solution is formulated as 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. In the authors considered a two-tier HWSN
- According to 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,” provides a new technique for finding fault tolerant with Quality of service.


### 2.3 EXISTING SYSTEM

Packet has not been dropped then the cluster head or the node which did not drop the packet behaves as a malicious node. As the cluster nodes and head will be in movement, the data can be sent more than one time. When the data reaches the processing head, the information will be checked and will be sent to the respective node destination. Now consider the information has been sent twice due to the movement in the cluster nodes and heads. As like the before process, the data will be reaching the processing head, the PC (processing center) will analyze the data, and identifies the data has been sent already to the respective receiver node. So the data will send the data again and again to a cluster head with the information that the data has been sent already. The data must reach the particular sender node as the data has been already sent, so the processing center can forward the data to the cluster heads, and from the cluster head the data will be forwarded to the respective cluster node. It supposes the data did not reach the source then the data must be dropped by some cluster head. The tradeoff issue between energy consumption vs. QoS gain 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 CH nodes may take a more critical role in gathering and routing sensing data. By this region, the life time of the time of a wireless sensor network will be minimized.

### 2.4 DISADVANTAGES OF EXISTING SYSTEM

- Provides Redundancy and Intrusion Problems in Data Transmission.
- The Current system does not provide redundancy reliability, timeliness, and security to maximize the system useful lifetime.
- It is difficult to detect extensive malicious attacks insidious attackers like packet dropping & bad mouthing attacks.
- No security for file transferring in the network.

When data need be sent from a sender to a receiver, then the data will go to the processing center. In WSN which consist of cluster head which will be a random based on the success ratio with a particular cluster. For each and every group of cluster a cluster head will be selected based on the success ratio. Then the router will maintain the multiple sensor nodes which are under them. If a sensor node is need to send some data to other sensor node. The sensor node will transmit the data to the cluster head. The packet will be dropped by head of the cluster, when the data has been already sent.

### 2.5 PROPOSED SYSTEM

A WSN must not only satisfy the application specific Quality of service (QOS) requirements such as reliability, timeliness, and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff issue between energy consumption vs. QOS gain becomes much more complicated when inside attackers or intruders are present in the network, as a path may be broken when a malicious node is on the path. The main goal of this paper is to exploit the tradeoff between energy consumption vs. the gain in reliability and security to maximize the system useful lifetime in the presence of attackers. The clustering of nodes is performed to increase the performance and decrease the energy consumption at each node. The energy efficiency is achieved by restricting the communication between inter cluster sensors which are far apart from each other and also by introducing a distributed intrusion detection system to detect and evict the malicious nodes causing certain types of energy consuming attacks. To satisfy the reliability requirement of a WSN, a modified multipath routing scheme is proposed. 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 at least 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 only to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. The existing works largely ignored the tradeoff between QOS gain vs. energy consumption which can adversely shorten the system lifetime. In the proposed work, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the WSN lifetime. Firstly, the reliability in data transfer is increased by eliminating the malicious nodes that are present in the network by employing distributed intrusion detection system. Compared with existing works cited above, our work is
distinct in that we consider redundancy management for both intrusion/fault tolerance through multipath routing technique and intrusion detection through voting-based IDS design to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes.

### 2.6 ADVANTAGES OF PROPOSED SYSTEM

- The Project provides a model-based analysis methodology by which the optimal multipath redundancy levels and intrusion detection settings may be identified for satisfying application QoS requirements while maximizing the lifetime of HWSNs.
- The clustering of nodes is performed to increase the performance and decrease the energy consumption at each node.
- Provides redundancy management & make as reliable data transmission in the network.
- Improves more network utilization i.e. provides maximum lifetime of the network.
- Provides load balancing for transferring the data security & bandwidth aggregation
  - Provides better performance in the presence of malicious nodes present in the network.
  - Security and reliability easily detect insidious attackers
  - Best intrusion detection in packet dropping, bad mouthing attacks.
- Multipath routing technique improves data delivery in Heterogeneous wireless sensor networks, and that will enforce secure, private and trustworthy networks.
- Energy efficiency is achieved by IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime.
- Intrusion detection through distributed voting based IDS design to maximize the system lifetime in the presence of unreliable & malicious nodes.
- Due to redundancy management the traffic loads in the network will be minimizes.

### III. ALGORITHMS AND FLOWCHARTS

#### 3.1 Algorithm for Dynamic Redundancy Management of Multipath Routing

1. **CH Execution:**
2. Get next event
3. **If** event is TD timer then
4. Determine radio range to maintain CH connectivity
5. Determine optimal TIDS, m, ms, mp by table lookup based on the current estimated density, CH radio range and compromise rate
6. Notify SNs within the cluster of the new optimal settings of TIDS and m
7. **else if** event is query arrival then
8. Trigger multipath routing using ms and mp
9. **else if** event is T clustering timer then
10. perform clustering
11. **else if** event is TIDS timer then
12. **for** each neighbor CH
13. **if** selected as a voter then
14. execute voting based intrusion detection
15. **else** / / event is data packet arrival
16. follow multipath routing protocol design to route the data packet.

#### 3.2 CH EXECUTION FOR DYNAMIC REDUNDANCY MANAGEMENT

1. **SN Execution**
2. Get next event
3. **If** event is TD timer then
4. Determine radio range to maintain SN connectivity within a cluster
5. **else if** event is control packet arrival from CH then
6. Change the optimal settings of TIDS, and m
7. **else if** event is T clustering timer then
8. Perform clustering
9. **else if** event is TIDS timer then
10. **for** each neighbour SN
11. **if** selected as a voter then
12. Execute voting based intrusion detection
13. **else** / / event is data packet arrival
14. Follow multipath routing protocol design to route the data packet.

*Sn Execution for Dynamic Redundancy Management*
3.3 Construction of Usecase plots

Use-case plots graphically depict scheme behavior (use cases). These plots deliver an eminent degree opinion of how the scheme is applied as opined from an outsider’s (actor’s) perspective. A use-case plot may depict all or approximately of the use cases of a scheme. Use-case plots graphically depict scheme behavior (use cases). These plots deliver an eminent degree opinion of how the scheme is applied as opioned from an outsider’s (actor’s) perspective. A use case plot may depict all or approximately of the use cases of a scheme.

3.4 A use-case plot behind contain:

- actors (“affairs” outside the scheme)
- use cases (scheme boundaries describing what the scheme ought do)
- Interactions or kinships among actors and use cases in the scheme admitting the associations, dependencies, and generalizations.

3.5 Kinships in use cases

1. Communication:

The communication kinship of an actor in a use case is shown by connecting the actor symbol to the use case symbol with a firm path. The actor is said to communicate with the use case.

2. Expends:

An Expends kinship among the use cases is shown by generalization arrow from the use case.

3. Extends:

The extend kinship is applied when we have one use case that is similar to approximately other use case but does a bit more. In heart it is like subclass.

Fig: Activity Diagram
3.7 Sequence Diagram

A sequence plot is a graphical opinion of a script that shows target interaction in a time-based sequence what happens commencing, what happens costing. Sequence plots establish the parts of objectives and help furnish necessity information to decide class duties and ports. At that depict are two main differences among sequence and collaboration plots: sequence plots show time-based target interaction while collaboration plots show how objectives associate with apiece other. A sequence plot has two dimensions: typically, vertical disrobing acts time and horizontal placement acts dissimilar objectives.

3.8 Class Diagram

A class is a set of objectives that share a mutual structure and mutual behavior (the same assigns, procedures, kinships and semantics). A class is an abstraction of real-world items. At that depict are 4 accesses as describing classes:

a. Substantive phrase access:
   b. Mutual class pattern access.
   c. Use case Driven Sequence or Collaboration access.
   d. Classes, Duties and collaborators Access.

3.9 Collaboration Diagram

A collaboration plot depicts interactions among objectives in conditions of sequenced messages. Collaboration plots redeliver a combination of information taken from class, sequence, and use case plots describing both the static structure and dynamic behavior of a scheme. It shows the target system as shown below. Here in collaboration plot the method call sequence is indicated by approximately numbering proficiency as shown below. The number indicates how the methods are called one later approximately other. We have taken the same order management scheme to depict the collaboration plot. The method calls are similar to that of a sequence plot. But the difference is that the sequence plot does not depict the target system where as the collaboration plot shows the target system. Collaboration plots extend a better opinion of a script than a Sequence plot when the examples is trying to understand all of the effects on a contribution target and are at that therefore good as procedural conception.

IV. MODULE CONCEPTION AND SYSTEM

The proposed system is divided into 4 different modules. First is the clustering and election of CH, where the clusters are dynamic to any changes and as well as the node with highest residual battery is considered as the current CH. The next module deals with the intrusion detection, where a distributed approach is used to identify and remove malicious nodes from the network. The last module deals with the redundancy management of multipath routing, where optimal amount of redundancy is identified for routing data.
4.1 MODULES

1. Clustering and Election of cluster head
2. Intrusion Detection and Eviction
3. Redundancy management of multipath routing
4. Energy consumption Analysis

1. Clustering and Election of cluster head:

Clustering techniques can aid in reducing useful energy consumption. Clustering can be extremely effective in one-to-many, many-to-one, one-to-any, or one-to-all (broadcast) communication. The essential operation in sensor node clustering is to select a set of cluster heads among the nodes in the network, and cluster the rest of the nodes with these heads. Cluster heads are responsible for coordination among the nodes within their clusters (intra-cluster coordination), and communication with each other and/or with external observers on behalf of their clusters (inter-cluster communication.)

2. Intrusion Detection and Eviction

Once all the connection setup is made, before the data transmission is started, the intrusion detection system is employed in order to detect and remove the malicious nodes in the network. If these malicious nodes go undetected, then those nodes can cause various kinds of attacks so that the battery of the sensor nodes is drained very soon. To detect compromised nodes, every node runs a simple host IDS to assess its neighbors. This host IDS is light-weight to conserve energy. It is also generic and does not rely on the feedback mechanism. It is based on local monitoring. That is, each node monitors its neighbor nodes only. Every authenticated system has a pair of authentication and node keys that are pre deployed in them. A node will take some data encrypted using its node key and sends it to the neighboring node present in the cluster, if in the case the neighbor is not an authenticated user, then he lacks the authentication key which is needed to decrypt this encrypted data. By now, the node will suspect the neighboring node as being malicious. But at this stage the node won’t be removed from the network, as the malicious behavior is not confirmed yet.

3. Redundancy management of multipath routing:

Multipath Routing is the method of establishing multiple paths between given source to destination nodes within the network. 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 at least 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 only to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. To improve lifetime of the sensor nodes and at same time to reduce amount redundancy in multipath routing, the optimal redundancy level is considered. Here multiple redundant sources are used for sensing the environment and then forwarding it to the respective CH. Depending upon the number of redundant sources, the level of reliability is increased by selecting more number of redundant paths. Thus achieving both reliable yet energy efficient data transfer.

Fig: Source and Path redundancy for a HWSN

4. Energy consumption Analysis:

Energy efficient protocols designed for sensors can increase the lifetime of the whole sensor network to a great extent. It is commonly believed that clustering is an effective solution for achieving scalability, energy conservation, and reliability. Using homogeneous nodes which rotate among themselves in the roles of cluster heads and sensor nodes leveraging CH election for lifetime maximization has been considered in the previous works. The energy efficiency is achieved here because of the reason that communication between long distance sensors is restricted to only the communication between the CHs of different clusters for inter cluster communication. Instead of spending more energy in communicating with node with large distance, the node directly communicate with its CH to forward the data. But in the proposed system, heterogeneous nodes used can further enhance performance and prolong the system lifetime.
IV. RESULTS

VI. CONCLUSIONS

In this paper we performed a tradeoff analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We developed a novel probability model to analyze the best redundancy level in terms of path redundancy ($mp$) and source redundancy ($ms$), as well as the best intrusion detection settings in terms of the number of voters ($m$) and the intrusion invocation interval ($TIDS$) under which 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, we applied our analysis results to the design of apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

REFERENCES


