International Journal For Technological Research In Engineering
Volume 1, Issue 11, July-2014 *ISSN (Online): 2347 - 4718*

RELIABLE AND ENERGY EFFICIENT MULTIPATH ROUTING FOR INTRUSION TOLERANCE IN WIRELESS SENSOR NETWORKS

Apoorva M[1], Hemanth S R[2]
[1]M.Tech, [2]Assi Prof, Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore
Mysore, India.

Abstract: ***Wireless sensor network (WSN) is group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment. WSNs are deployed in an unattended environment in which energy replenishment is very difficult. Due to limited resources, 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. 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.***

Keywords: ***Wireless sensor networks, energy efficiency; reliability; clusters; intrusion detection, multipath routing.***

I. INTRODUCTION

The wireless sensor networks (WSNs) are usually 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 (Quality of Service) requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. It is believed that clustering is an effective solution for achieving scalability, energy conservation, and reliability. Homogeneous clusters [1] consisting of cluster head (CH) and sensor nodes (SN) were usually used for lifetime maximization. But heterogeneous nodes can further enhance performance and prolong the system lifetime, as nodes with superior resources serve as CHs performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. 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 environments in which CH nodes may take a more critical role in gathering and routing the sensed data. Thus, very likely the system should employ an intrusion detection system (IDS) with the goal to detect and remove malicious nodes. Multipath routing [2] 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. Most of the prior researches have focused on using multipath routing to improve reliability and only some attention has been paid to using multipath routing to tolerate insider attacks, but largely ignored the tradeoff between QOS gain vs. energy consumption which can adversely shorten the system lifetime. The main objective is to address the tradeoff 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, 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. Also, a voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. Majorly the optimal multipath redundancy levels are identified along with the intrusion detection settings for satisfying the application QOS requirements while maximizing the lifetime of HWSNs are designed. For the issue of 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.

A. Multipath Routing in Wireless Sensor Networks

The limited capacity of a multi-hop path and the high dynamics of wireless links, single-path routing approach is unable to provide efficient high data rate transmission in wireless sensor networks. Nowadays, the multipath routing approach is broadly utilized as one of the possible solutions to cope with this limitation. The main design issues in the

development of the existing multipath routing protocols are discussed below.

B. Motivations for Using Multipath Routing Approach in Wireless Sensor Networks

Routing technique has demonstrated its efficiency to improve wireless sensor network's performance. In the following, the performance gains that can be achieved using multipath routing approaches are discussed.

C. Reliability and Fault-Tolerance

The time-varying characteristics of low-power wireless links, dynamic network topology, and wireless interference, make reliable data transmission in wireless networks a challenging task. The idea behind using multipath routing approach in wireless sensor networks was to provide path resilience and reliable data transmission. In the fault tolerance domain, whenever a sensor node cannot forward its data packets towards the sink, it can benefit from the availability of alternative paths to salvage its data packets from node or link failures. Through this mechanism, as long as an alternative path is available from a target area towards the sink node, data forwarding can be continued without any interruption even in the case of path failure. Multiple paths also can be used simultaneously to elevate data transmission reliability.

There are two different approaches to provide reliable data transmission through concurrent multipath routing. The first approach is based on transmitting multiple copies of an original data packet over different paths to ensure packet recovery from several path failures. Through this technique, data transmission reliability can be guaranteed, if data forwarding over at last one path is done successfully. Based on the utilized coding technique, each source node adds some additional information to the original data packets and then distributes the generated data packets over different paths. To reconstruct original packets, at last a certain number of transmitted data packets from each source node should be received by the sink node.

D. Load Balancing and Bandwidth Aggregation

Intensive traffic loads in high-data rate applications are prone to congestion, which highly influences the network performance. To handle this problem, wireless sensor networks can use multipath routing to increase network capacity by employing more network resources. Multipath routing approaches can provide the best solution to support the bandwidth requirements of different applications and reduce the probability of network congestion through splitting network traffic over several paths.

E. QOS Improvement

QOS support in terms of reliability, security and data delivery is an important objective in designing multipath routing protocols for different types of networks. Discovered paths with various characteristics can be utilized to distribute network traffic based on the QOS demands of the application for which the multipath routing protocol has been designed. For instance, the level of redundancy can be increased as the criticality of the data increases. By doing so we can reduce energy wastage for less critical data transfers, at the same time use more number of paths for the data that is been sensed from more number of redundant source sensors. The reliability of data transfer is increased by forwarding data through more than one paths, believing that it reaches destination at least through any one of them. Furthermore, in contrast with the single-path routing techniques multipath routing approaches can preserve QOS demands of the intended application in the case of path failures through directing network traffic to the another active path.

II. METHODOLOGY

The proposed system is divided into 3 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. The methodology used in the implementation of each of these modules is explained in the further section.

A. Clustering and Election of cluster head

Sensor nodes are typically less mobile and more densely deployed than mobile ad-hoc networks. Sensor nodes are usually left unattended e.g., in hostile environments, which makes it difficult or impossible to re-charge or replace their batteries. This necessitates devising novel energy-efficient solutions to some of the conventional wireless networking problems. Exploiting the tradeoffs among energy, accuracy, and using clusters are important techniques for prolonging network lifetime. Clustering sensor nodes is an effective technique for achieving these goals. Network lifetime can be defined as the time elapsed until the first node in the network depletes its energy. Energy consumption in a sensor node can be due to either "useful" or "wasteful" sources.

Useful energy consumption can be due to

(i) Transmitting/ receiving data.

(ii) Processing query requests.

(iii) Forwarding queries/data to neighboring nodes.

Wasteful energy consumption can be due to

(i) Retransmission due to packet collisions.

(ii) Overhearing.

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).

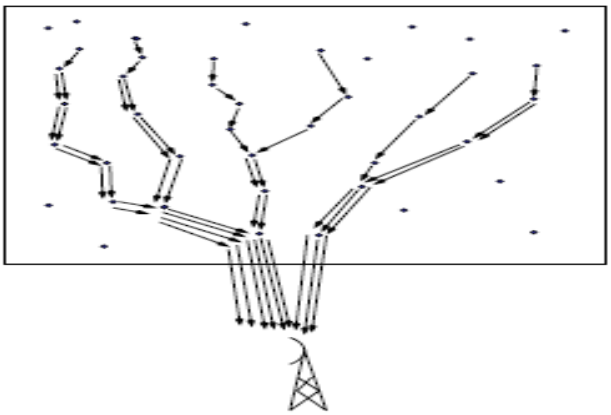

Fig 1: Multi-hop forwarding without clustering.

Figure 1 depicts an application where sensors periodically transmit information to a remote observer (base station) when there are no clusters formed. There is a lot of energy wastage in all the sensor nodes involved in communication, which intern causes a network overhead as well.

The Figure 2 shows how clustering can reduce the communication overhead for multi-hop networks. With clustering, nodes transmit their information to their cluster heads. A cluster head aggregates the received information and forwards it over to the observer. Periodic re-clustering can select nodes with higher residual energy to act as cluster heads. Network lifetime is prolonged through (i) Reducing the number of nodes contending for channel access,(ii) Summarizing network state information and updates at the cluster heads through intra-cluster coordination, and (iii) Routing through an overlay among cluster heads, which has a relatively small network diameter.

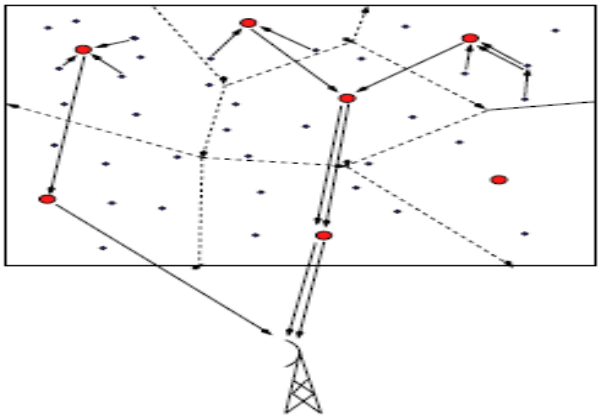

Fig 2: Multi-hop forwarding with clustering.

In order to balance the energy consumption in entire network, the node having the highest battery level will be selected as a cluster head (CH). In order to do so, the nodes in a cluster will broadcast their battery levels to all the nodes in cluster. Later the node with the highest remaining battery level is chosen. The selected cluster will then broadcast its details to the rest of the sensor nodes, which can be used for further communications with the cluster head. To keep track of all the nodes that are present in the vicinity of a cluster, every node keeps broadcasting the advertisement packets. If in case a node is down due to power depletion or any other reason, then its neighboring nodes will not get any reply packets from this node. A preset counter value will be initially assigned to every neighboring node after getting a reply packet from it. If in case the node does not reply, then this counter value will be decremented by 1 each time when there is no reply. Finally when the counter value reaches 0, the node will be considered dead and will be removed from the cluster. Further, no more data transfer will take place between this node and any other nodes in the cluster.

B. 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. To remove malicious nodes from the system, a voting based distributed IDS is applied periodically. A CH is being assessed by its neighbor CHs, and a SN is being assessed by its neighbor SNs. Each time, neighbor nodes around a target node will be chosen as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node. To preserve confidentiality, we assume that the WSN executes a pair wise key establishment protocol after deployment. Thus, when SNs join a new cluster, the CH node will have pair wise keys with the SNs joining its cluster. Since every SN shares a pair wise key with its CH, a SN can encrypt data sent to the CH for confidentiality and authentication purposes. Every CH also creates a pair wise key with every other CH. Thus a pair wise key exists for secure communication between CHs. This mechanism is useful to prevent outside attackers, not inside attackers. The *m* voters share their votes through secure transmission using their pair wise keys. When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted.

C. Pair wise key Exchange for secure communication

Though an intrusion detection system is been proposed for detecting and removing the inside attackers, it is also very essential to secure the communication from the outside attackers. In order to protect the communication from outside attackers the data has to be encrypted before transferring. To

perform encryption/decryption a pair wise key exchange of public key is performed between every pair of CH and sensor nodes and along between every pair of CHs. Whenever data has to be sent from a sensor node to a CH, the sensor node encrypts the data with CH's public key and send. Whenever the data has to be decrypted back, the CH will use its own private key to decrypt the data. The RSA public key cryptography is used in the project to satisfy this security requirement. Security requirements of WSNs are similar to conventional computer networks, therefore parameters such as confidentiality, integrity, availability and authenticity must be taken into account in creation of a network environment. Due to limitations of WSNs, not all security solutions designed for conventional computer networks can be implemented directly in WSN. For a long time, it was believed that the public key cryptography was not suitable for WSNs because it required high processing power, but through studies of encryption algorithms RSA was verified as a feasible technique for WSNs. The RSA cryptographic algorithm is currently the most used among the asymmetric algorithms, working from the difficulty of factoring large prime numbers. The RSA cryptographic algorithm is public, making the node to share its public key with all the other nodes and it is the key that is used for encrypting data. Secrecy is the key that has the function to parameterize the cryptographic function, i.e. only with the key any one can encrypt or decrypt a message. Another important factor is that the key has the ability to change the output of the algorithm, so every change of key in cryptographic algorithm generates a new encrypted message. The key size is critical, because t longer the key, more work it will be to the crypto analyst to try to decipher the message. In general, keys have sizes of 64, 128 or 256 bits and may be higher or lower, according to security needs.

Currently, in addition to confidentiality, encryption also operates in the fields of integrity of authentication and is described below:

- *Confidentiality:* ensuring that only the sender and receiver have the ability to understand the message being exchanged.
- *Integrity:* Ability to check if a message was altered during transmission.
- *Authentication:* Medium to prove the identity of an individual communication.

Encryption is the standard method for defending a WSN of most possible attacks, and the various levels of encryption implicate variations in overhead in the form of growth in the size of the package data, code size, processor usage, memory. The cryptographic methods used in WSN should meet the constraints of computational devices, and go through evaluation before being implanted. Public key cryptosystem security is based on the difficulty to be factoring large prime numbers. Through this RSA technique is used to encrypt data and to create digital signatures.

It was so successful that today is the RSA public key algorithm used most in the world. The encryption scheme uses RSA and for the fact that:

$m^e \equiv m(mod\ n)$ *(1)*

Equation (1) represents an equation used for encrypting the message 'm' using the values of 'e' and 'n' which results in the cipher text 'c'. The decryption works by using the equation shown below:

$c^d \equiv (m^e)^d \equiv m\ (mod\ n)$ *(2)*

Equation (2) shows how the cipher text 'c' can be decrypted back to get the original message 'm'. Here the value of'd' is used along with 'n' to perform decryption. The safety lies in the difficulty of computing a clear text m from a cipher text. The RSA scheme is a block cipher. Each plaintext block is an integer between 0 and n – 1 for some n, which leads to a block size ≤ log2 (n). The typical size for n is 1024 bits. The details of the RSA algorithm are described as follows.

1) Pick two large prime numbers p and q such that $p \neq q$;
2) Calculate $n = p \times q$;
3) Calculate $\Phi(n) = (p-1)(q-1)$;
4) Pick e, so that $\gcd(e, \Phi(n)) = 1$, $1 < e < \Phi(n)$;
5) Calculate d, so that $d \cdot e \bmod \Phi(n) = 1$, *i.e.*, d is the multiplicative inverse of e in mod Φ(n);
6) Get public key as $K_U = \{e, n\}$;
7) Get private key as $K_R = \{d, n\}$.

For encryption, consider plaintext block P < n, its cipher text is $C = P^e \bmod n$. For decryption, consider cipher text block C, its plaintext is $P = C^d \bmod n$.

RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to Φ (n), has exponential inverse in mod n. Its exponential inverse d can be calculated as the multiplicative inverse of e in mod Φ (n). The premise behind RSA's security is the assumption that factoring a big number (p and q) is hard. And thus it is difficult to determine Φ (n). Without the knowledge of Φ (n), it would be hard to derive d based on the knowledge of e.

D. Redundancy management of multipath routing

Even after employing the intrusion detection system, there might be some undetected malicious node present in the network. These nodes can once again cause attacks, so that the packets will not reach the destination in a correct form. In order to make sure that the data reaches the destination at any cost, multipath routing is used to forward data packets to destination. In multipath routing, the same data will be sent from multiple paths to the same destination, believing that data reaches safely at least through one of the several paths. The two types of redundancies namely, source and path redundancies are applied to increase the reliability of data transfer. Here, increasing the source or path redundancy enhances reliability and security. However, it also increases the energy consumption, thus contributing to the decrease of the system lifetime. Thus, there is a tradeoff between reliability/security gains vs. energy consumption. The distributed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily wasting energy so as to maximize the query success probability and the system lifetime. For redundancy management, we create *mp* paths between the source CH and the PC for path redundancy. The *mp* paths are formed by choosing *mp* CHs in the first hop and then choosing only one CH in each of the subsequent hops.

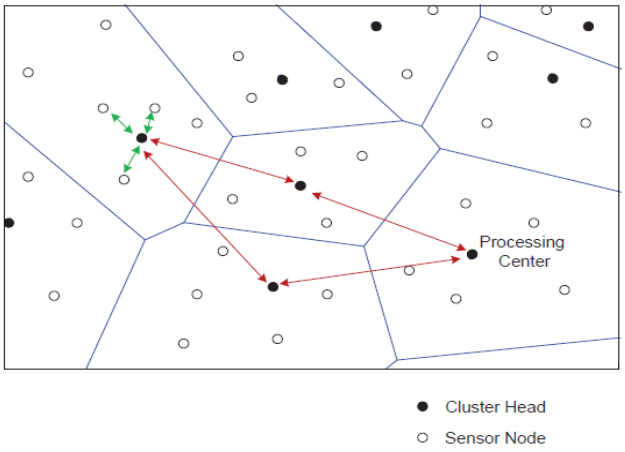

Fig 3: Source and Path redundancy for a Heterogeneous WSN.

The Figure 3 shows a scenario with a source redundancy of 3 (*ms* = 3) and path redundancy of 2 (*mp* = 2).To route the information between nodes, no path information is maintained. The location of the destination node needs to be known to correctly forward a packet. As part of clustering, a CH knows the locations of SNs within its cluster, and vice versa. A CH also knows the location of neighboring CHs. For identifying the possible paths from source to the destination, the cluster head of the sending cluster will send the data transfer request packet to the next immediate cluster head. Each of the request packets will contain the details of the packet like type, destination and source address. Every node will compare its own IP address to that of the packet's destination IP address, if they don't match, it just adds its IP address to packet and then forward it further. Once the destination IP address matches with the node's address, it gets to know that it is the receiver and it receives the data and send the reply packet back. In order to send the reply packet to the sender, the list of IP addresses that was available the request packet will be used in the reverse order to reach the sender back. Now, the sending cluster head will end up with a list of paths reaching the destination from the current source. Next the count of the number of redundant sources that are sensing the environment in the sender cluster is obtained. In order to find the optimal number of paths to use for data transmission and to reduce the energy consumption of using multipath routing, the paths which have the number of hops either lesser or equal to number of redundant sources will be selected. The rest of available paths reaching the destination having more hops than the number of redundant sources will be discarded and it won't be used for data delivery. By doing so, the amount of redundancy employed is reduced up to some level and also at the same time it conserves a lot of energy in many of the sensor nodes that were present in the rejected paths. The objective of dynamic redundancy management is to dynamically identify and apply 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 to maximize MTTF, in response to environment changes.

III. PERFORMANCE ANALYSIS

The performance of the system is based on the achieved energy efficiency and the reliability of the data transfer in the presence of malicious nodes. The results obtained from the proposed system are much better than the existing system in terms of energy conservation and gain in reliability. Also the security of the data transfer is achieved by using RSA algorithm for encrypting/decrypting the data in the network during data transfer.

A. Energy consumption Analysis

A wireless network consists of very large number of small, relatively inexpensive and low-power sensors. Because of the fact that each node has only limited energy resource and the battery power and it is practically not possible to replace battery every now and then. However, the energy constraint is unlikely to be solved soon due to slow progress in developing battery capacity. So an efficient algorithm which can use energy for a larger lifetime is adopted in the proposed work. The goal is to minimize the energy spent for delivering a packet from source to destination. 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. In heterogeneous clustering, nodes with superior resources serve as CHs performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. So to reduce the energy consumption, the nodes with the highest amount of residual battery level is selected as CH. By doing so, we try to avoid the case of randomly selecting a CH which might be having much lesser power than that is required to perform computations in a WSN. Also, the usage of intrusion detection and eviction system before performing data transfer will reduce the energy wastage that could have happened if those undetected intruders were present in the network causing energy consuming acts. Lastly, the modified multipath routing scheme used is much better than the other existing multipath routing protocols by the fact that it avoids data forwarding through all possible paths from the source to the destination and also the path consisting of large number intermediate hops are usually avoided depending upon the criticality of data transfer. A query response propagates over SNs for source redundancy (m_s) and over CHs for path redundancy (m_p). Hence, m_s directly affect energy

consumption of SNs and m_p directly affects energy consumption of CHs. But introducing heterogeneity in clusters, energy consumption can be balanced between the nodes of the cluster thus increasing the system useful lifetime of the sensor networks.

B. Reliability gain

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. The intrusion free paths are obviously more reliable than the paths consisting attackers which could increase the probability of data loss. Further to increase the reliability of the data transfer, multipath routing is used. But this is more energy consuming as it involves multiple paths and all the sensor nodes that are present in that path will be subjected to energy depletion. 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.

IV. CONCLUSION AND FUTURE WORK

In this proposed work, a tradeoff analysis of energy consumption vs. QOS gain in reliability, timeliness, and security for redundancy management of clustered wireless sensor networks utilizing multipath routing to answer user queries was performed. The best redundancy level in terms of path redundancy and source redundancy, as well as an intrusion detection system satisfying the reliability and security requirements of query processing applications in the presence of malicious nodes is analyzed. Finally, the analysis results are applied to design a dynamic redundancy management algorithm to identify and the best number of redundant paths to be used for data transfer. It is made dynamic to response to the environmental changes to prolong the system lifetime. For future work, we can explore more extensive malicious attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

REFERENCES

[1] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks" 22nd Conf. of IEEE Computer and Communications, 2003, pp. 1713-1723.

[2] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM:reliable information forwarding using multiple paths in sensor networks," 28th IEEE Local Computer Networks, Bonn, Germany, 2003, pp. 406-415.

[3] Waldir Ribeiro Pires Junio, Thiago H. de Paula Figueiredo and Hao Chi Wong "Malicious Node Detection in Wireless Sensor Networks" Proceedings of the 18th International Parallel and Distributed processing Symposium (IPDPS'04), Santa Fe, New Mexico, April 26-30 2004.

[4] 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," 1st ACM Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, vol. 29, pp. 216-230, 2006.

[6] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320-1330, 2006.

[7] 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 Comput, vol. 5, no. 6, pp. 738-754, 2006.

[8] Tanveer Zia and Albert Zomaya," Malicious Node Detection by a Monitoring Mechanism in Wireless Sensor Networks," In the proceedings of the IEEE INFOCOM 2006 Students Workshop, Barcelona, Spain, April 23-24, 2006.

[9] Ye Ming Lu and Vincent W. S. Wong "An energy-efficient multipath routing protocol for wireless sensor networks". International journal of communication system, Vancouver, Canada, 2007.

[10] 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.

