Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Redundancy Management of Multipath Routing for Intrusion Tolerance of Packet Loss by Malicious Node in HWSN

Mr. Digamber T. Bodake
ME Computer & Late G.N. Sapkal COE,
Nashik, Maharashtra, India

Prof. Nilesh R. Wankhade
HOD Computer & Late G.N. Sapkal COE,
Nashik, Maharashtra, India

Abstract— In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs) where we are utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes which cause packet loss in the network. The research problem we are addressing in this paper is efficient redundancy management of multipath routing in a clustered Heterogeneous Wireless Sensor Network to tolerate intrusions which are responsible for packet loss and jamming attack. The main goal and objective of the paper is to use redundancy management on multipath routing to tolerate and detect intrusions. The key concept of our redundancy management is to achieve the balance between energy consumption and gain in reliability, timeliness along with the security to maximize the system useful lifetime. In our work we have considered redundancy management of multipath routes which are based on trust and energy values and it is used for intrusion detection as well as to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. In this paper we are using symmetric encryption technique to protect confidentiality. To increase security we discovered more extensive attacks by the malicious nodes such as packet dropping attack and jamming attacks, each attack is having different energy requirement as well as security and reliability.

Keywords— Heterogeneous Wireless Sensor Networks, Intrusion Detection, Malicious Node, Multipath Routing, Packet Loss.

I. INTRODUCTION

A. Detail Problem Definition

Many wireless sensor networks (WSNs) are deployed at the environment where the energy replenishment is very difficult but it is not impossible. In WSN there are limited resources which are not only used to satisfy QoS requirement but also they must be useful to increase system lifetime with minimum energy consumption. So our aim is to solve the problem of balance between energy consumption and QoS requirement to provide reliability gain with the goal to maximize the WSN system lifetime. This problem is well explored in literature. However, in literature no work exists to consider the trade-off in the presence of malicious node which are responsible for packet loss also which are harmful to the network. It is considered that clustering is one of the best solutions to achieve the scalability, reliability and energy conservation in wireless sensor network. If the homogeneous network is consider then the cluster head (CH) is selected among all nodes which rotate in the network. Some of the protocol like HEED [2] is used to elect cluster head among all available nodes in the network, which useful for lifetime maximization. Modern studies as given in [5][7] suggest that use of heterogeneous nodes can also enhance performance in better way and prolong the system lifetime in HWSN. The nodes where highest resources such as highest residual energy is available will perform the role of CH and they are useful to perform computationally intensive task while inexpensive less capable SNs are utilized mainly for sensing the environment.

B. Justification of Problem

The steadiness between energy consumption with QoS requirement for reliability gain becomes much more difficult to manage when there is an inside attacker available in the network. This inside attacker will attack the sensor node and act as a malicious node and will be responsible to break the path in the network and will disturb the working of the network. This is the case which generally happens in heterogeneous WSN (HWSN) environments where CH nodes takes more critical role in routing as well as data gathering from the sensor nodes(SN) which are available in the network. Thus, it is essential to employ effective intrusion detection system (IDS) to detect as well as to remove such malicious nodes from the system. Also such IDS system must provide good performance with minimum energy consumption so that it is helpful to improve system lifetime. While in the literature there are number of intrusion detection techniques for WSN like [8][12], but the issue is how often the intrusion detection should be invoked to detect and remove malicious node from the system so that we can improve system useful lifetime. The issue is exclusively precarious for energy-constrained WSNs designed to stay alive for a long mission time.

Another solution to increase system lifetime is to use multipath routing which is also for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is to increase the number of path toward the sink from every node

available in the WSN. That is we need to enlarge the count of number of path reaching the sink node or base station. While most prior research focused on using multipath routing to improve reliability [3], [4], [14], some attention has been paid to using multipath routing to tolerate insider attacks [15][17]. All the current studies, however, largely ignored the steadiness between QoS gain and energy consumption which can adversely shorten the system lifetime

C. Need of Proposed System

The problem we are addressing in this paper is effective redundancy management of a clustered HWSN to maximize system lifetime operation in the presence of unreliable and malicious nodes which are responsible for packet loss. We are addressing the trade-off issue between energy consumption with QoS requirement to gain in reliability and timeliness as well as to increase security so that we can maximize the lifetime of a clustered heterogeneous WSN, it will also be a satisfying application for QoS requirements in case of multipath routing.

More specifically, we are analysing the optimal amount of redundancy in WSN through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the probability to answer users query must be maximized while maximizing the system lifetime.

For the issue of intrusion tolerance through multipath routing, there are two major problems to solve first is how many paths to use and second is what paths to use. We are focusing on to address the how many paths to use to reach to the sink problem. Our approach is different from existing for the, what paths to use problem, in that we do not consider specific routing protocols (e.g., MDMP for WSNS or AODV for MANETs), nor the use of feedback information to solve the problem. Rather, we are employing a IDS by which intrusion detection is performed only locally so that there must be less energy conservation by the nodes in the network. The compromised nodes are detected and the path through that node is ignored from the heterogeneous WSN. In this paper we decide how many paths to use in order to tolerate residual compromised nodes that survive our IDS, so as to increase system useful lifetime of the HWSN.

The contribution of our paper is that we explore more extensive malicious attacks in addition to packet loss attack and jamming attacks which occur because of packet dropping by malicious nodes, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

II. RELATED WORK

A. Study of Existing Techniques

If you are using Word, O. Younis and S. Fahmy proposed HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, In this the author propose a novel distributed clustering approach for long-lived ad hoc sensor networks. The proposed approach does not make any assumptions about the presence of infrastructure or about node capabilities, other than the availability of multiple power levels in sensor nodes. Authors present a protocol, HEED (Hybrid Energy-Efficient Distributed clustering), that periodically selects cluster heads according to a hybrid of the node residual energy and a secondary parameter, such as node proximity to its neighbours or node degree.

E. Felemban et al. Proposed MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks, In this paper, author present a novel packet delivery mechanism called Multi-Path and Multi-SPEED Routing Protocol (MMSPEED) for probabilistic QoS guarantee in wireless sensor networks. The QoS provisioning is performed in two quality domains, namely, timeliness and reliability. Multiple QoS levels are provided in the timeliness domain by guaranteeing multiple packet delivery speed options. In the reliability domain, various reliability requirements are supported by probabilistic multipath forwarding.

I. R. Chen et al. proposed Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks, n 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.

H. M. Ammari et al. proposed Promoting heterogeneity, mobility, and energy aware Voronoi diagram in wireless sensor networks system, To solve the energy sink-hole problem for homogeneous WSNs, author propose a localized energy-aware-Voronoi-diagram-based data forwarding (EVEN) protocol. EVEN combines sink mobility with a new concept, called energy-aware Voronoi diagram.

S. Bo, L. Osborne et al. proposed Intrusion detection techniques in mobile ad hoc and wireless sensor networks, In this paper, first author briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. Then, they focus on their intrusion detection capabilities. Specifically, they present the challenge of constructing intrusion detection systems for mobile ad hoc networks and wireless sensor networks.

J. H. Cho, et al. proposed Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks, In this paper, they analyse the effect of intrusion detection system (IDS) techniques on the reliability of a mission-oriented group communication system consisting of mobile groups set out for mission execution in mobile ad hoc networks. Unlike the common belief that IDS should be executed as often as possible to cope with insider attacks to prolong the system lifetime, author discover that IDS should be executed at an optimal rate to maximize the mean time to failure of the system.

Y. Zhou, Y. Fang, and Y. Zhang, proposed Securing wireless sensor networks: a survey In this paper, author present a comprehensive survey of WSN security issues that were investigated by researchers in recent years and that shed light on future directions for WSN security.

H. Su and X. Zhang, proposed Network lifetime optimization for heterogeneous sensor networks with mixed communication modes, In this paper, author consider the cluster-based heterogeneous WSNs, which consist of two types of nodes, namely, the powerful cluster-heads and the inexpensive sensor nodes. In particular, in the WSN, the sensor nodes are deployed along the grid points. To better balance the energy consumption, the sensor nodes exchange data with the cluster-heads.

I. Slama, B. Jouaber, and D. Zeghlache, proposed optimal power management scheme for heterogeneous wireless sensor networks: lifetime maximization under QoS and energy constraints, In this paper, author propose a power- and-QoS based framework for heterogeneous sensor networks. This framework is formulated as an optimization problem. It aims at maximizing the application lifetime while ensuring acceptable level of quality of service.

R. Machado, et al. proposed Adaptive density control in heterogeneous wireless sensor networks with and without power management; the authors study the design of heterogeneous two-tier wireless sensor networks (WSNs), where one tier of nodes is more robust and computationally intensive than the other tier. The authors find the ratios of densities of nodes in each tier to maximize coverage and network lifetime.

E. Stavrou and A. Pitsillides, proposed A survey on secure multipath routing protocols in WSNs, In this paper author focus at security issues concerns in WSNs and present a matrix that analysed the security factor provided by the secure multipath routing protocols in wireless sensor networks.

T. Shu, M. Krunz, and S. Liu, proposed Secure data collection in wireless sensor networks using randomized dispersive routes, In this paper, authors study routing mechanisms that circumvent (bypass) black holes formed by these attacks. They argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes.

B. Analysis of Existing System

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 tradeoff in the presence of malicious node.

In Existing systems:-

- In existing works no consideration was given to the existence of malicious node.
- In existing works no consideration was given to Energy Consumption & detection of Compromised node for Intrusion Detection.
- In existing works no consideration was given to Packet dropping & Bad Mounting attacks by Compromised node & Energy Consumption & Maximization of WSN lifetime.

C. Comparison of existing systems with proposed system

In Existing System, effective redundancy management of a clustered HWSN is used to prolong its lifetime operation in the presence of unreliable and malicious nodes. We 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, 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.

III. METHODOLOGY

A. Concept

In the Proposed System we are addressing efficient redundancy management of a clustered HWSN to maximize system lifetime operation in the presence of unreliable and malicious nodes which are responsible for packet loss. We are addressing the balance between energy consumption with the QoS requirement to gain in reliability and timeliness as well as to increase security so that we can maximize the lifetime of a clustered heterogeneous WSN, it will also be a satisfying application for QoS requirements in case of multipath routing.

In our work we have considered redundancy management of multipath routes which are based on trust and energy values and it is used for intrusion detection, and to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. Today's research challenge in WSNs is coping with low power communication. Routing protocols in this regard plays a key role in efficient energy utilization. In sending data from sensor nodes to BS there is need to select a specific route and must be a shortest route, which mange to minimize the energy consumption is necessary. Hence we are using clustering approach to minimize the energy consumption. In this paper we are using symmetric encryption technique to protect confidentiality. To increase security we have revealed more extensive attacks by the malicious nodes such as packet loss attack and jamming attack each assault is having altered energy requirement as well as security and reliability. Specifically, we are analyzing the optimal amount of redundancy in WSN through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the possibility to answer users query must be maximized while maximizing the system lifetime

To tolerate intrusion through multipath routing, there are two major problems to solve first is how many paths to use and second is what paths to use. We are concentrating on to report the how many paths to use to reach to the sink problem. Our approach is different from existing for the, what paths to use problem, in that we do not consider specific routing protocols and we are not using any feedback information to solve the problem. Rather, we are employing IDS by which intrusion detection is performed only locally so that there must be less energy conservation by the nodes in the network. The compromised nodes are detected and the path through that node is ignored from the heterogeneous WSN. In this paper we decide which paths to use in order to tolerate residual compromised nodes that survive our IDS, so as to increase system useful lifetime of the HWSN.

In this paper we also discover more extensive malicious attacks in addition to packet loss and jamming attacks which occur because of malicious nodes, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

B. System Model

A heterogeneous WSN consists of different types of sensors having different sensing capabilities. We have considered two types of sensor nodes, one is cluster head (CHs) and another is sensor node SNs. Cluster heads (CHs) are more superior than sensor nodes(SNs) in consideration of energy as well as computational resources. We are using heterogeneous network in which each node is having more amount of resources.

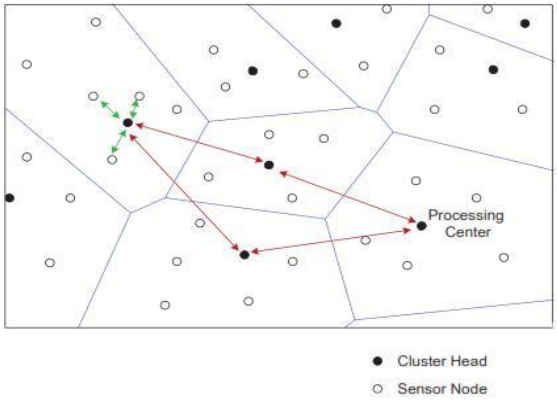

Fig 1. System Model

Redundancy management of multipath routing for intrusion tolerance in presence of malicious nodes is achieved through two forms of redundancy: (a) source redundancy by which *ms* SNs sensing a physical phenomenon in the same feature zone are used to forward sensing data to their CH (referred to as the source CH); (b) path redundancy by which *mp* paths are used to relay packets from the source CH to the base station through the use of neighbouring CHs. Fig.1 shows a scenario with a source redundancy of 3 (m=3) and a path redundancy of 2 (m=2). It has been reported that the number of edge-disjoint paths between nodes is equal to the average node degree with a very high probability. Therefore, when the density is adequately high such that the average number of one-hop neighbours is sufficiently larger than *mp* and *ms*, we can effectively result in m redundant paths for path redundancy and *mp* distinct paths from m sensors for source redundancy.

We are assuming that geographic routing which is a well-known routing protocol for WSNs, is used to route the data from CH to the base station or sink along with multipath routing; thus, in this case there is no need to conserve path information of the network. We must know the location of the destination node so that we can correctly send the packet towards it. So the CH are responsible to get the location of all SN and vice versa in its cluster and it is the part of clustering. A CH is also aware with the location of neighbour CHs along with the direction towards the base station or sink.

In this paper we are using clustering to reduce the energy consumption by the nodes to send data to the base station. Cluster is the group of Nodes and in the paper, we are grouping the nodes to form cluster. Here cluster formation is based on the specific region and the nodes located in the specified region. We are selecting the region with specific distance from the base station and then the area is selected and the nodes inside region are located and grouped. In this approach clusters are formed statically at the time of network deployment so all the sensor nodes and their CH nodes are selected. The Cluster Head is selected on the Highest Energy basis, the node which has maximum energy is selected as Cluster Head.

We also assume that all the sensor nodes and cluster heads should operate in power saving mode so that less energy is utilized. Hence, a sensor is either active i.e. transmitting or receiving or it is in sleep mode. For the energy consumption while sending & receiving information we are using the energy model in [2] for both CHs and SNs.

To preserve confidentiality we are using AES symmetric key encryption algorithm. AES is Symmetric key Cryptographic algorithm. It is used to provide security in our paper. While sending data, a sensor node can encrypt data by using key encryption technique and then send that encrypted data to the CH so that it is helpful to achieve confidentiality and authentication. Then the data is transmitted and it will help to secure data from the attacker and packets are formed from the file and actually packets are transmitted. At the destination the data is decrypted by the destination node.

To detect compromised nodes from HWSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The acknowledge ACK which is received is compared with the size of received data; if it is equal then data is forwarded successfully with no loss in packets; otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens. This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN.

To detect jamming attack in network we are using a counter based approach if the counter goes beyond the threshold then it will detect that network is jammed. Here we have noted that increasing source redundancy as well as path redundancy will enhances the reliability and security. However, it also decreases the energy consumption and thus it contributing to the increase of the system lifetime. Thus, there is balance between gain in reliability and security with the less energy consumption. The dispersed 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.

C. Algorithm for Intrusion Tolerance & Attack Detection

```
1:  if(network created)
2:  if(SourceNode != DestNode)
3:      int  Size = datasize;
4:      Send(data)
5:          ACK = data received size;
6:          if(ACK == datasize)
7:            Data received successfully;
8:            Flag = true;
9:          else
10:          Data is lost in path;
11:          Flag  = false;
12: if(Flag == false )
13:    For all paths;
14:        Calculate average of energy and trust value.
15:        if(average==maximum value)
16:            shortest path = current path;
17:  Send(data);
```

In proposed work, we are using multipath routing and encryption/Decryption technique. The fundamental obligation of the sensor nodes in each system is to sense the range and transmit their gathered data to the sink node for further operations. Multipath Routing is a routing procedure, which chooses various ways to convey information in the middle of source and destination nodes. As the essential significance of routing means, selecting best way in the system, multipath routing strategies are utilized to choose the best path in the network.

From the above algorithm, Firstly a network is created which consist of different clusters and based on energy levels of each node the cluster heads are elected. To forward a data within a HWSN distinct source node and destination nodes are selected. To increase system lifetime we have to detect malicious nodes which are responsible for different attacks such as packet loss and jamming attack. To detect compromised nodes from HWSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The ACK is compared with the size of received data; if it is equal then data forwarded successfully with no loss in packets; otherwise it will detect loss in the packet. Hence, it detects such a node as a malicious node due to which packet loss happens. This is applied to every node in the network and each node will assess its acknowledgement with the size of data received to detect the attack and compromised node in the WSN.

IV. RESULTS AND DISCUSSION

The aim of our system is to increase lifetime and security in the network. To evaluate the performance we need to use different metrics. In our work we are using following metrics:

- Data Transfer Time
- Data Delivery Ratio

The following graph of data transfer time required for communication, in this graph we shows three types of communication with Jamming, with MIM attack and with Normal communication and the time required for the communication. Lifetime is depending on the Energy of the network and as the energy consumption depends on the node processing time. The jamming attack and MIM attack requires more time for processing and it consumes more energy and If we are using the same path for communication then we are wasting unnecessary energy and hence node may cause dead hence to avoid this we are changing the path and after the path change the data transfer time is less as compared to attack. Hence the minimum time requires minimum energy and indirectly the network lifetime is increased by path changed for communication.

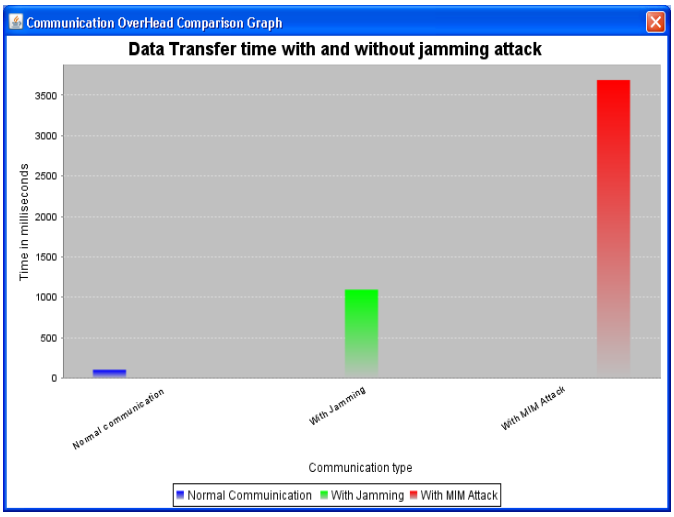

Fig2: Data Transfer Time

The table shows the comparison values between three types of communication with Jamming, with MIM attack and with Normal communication and the time required for the communication.

TABLE I DATA TRANSFER TIME

Algorithms	**Data Transmission Time**
MIM attack	3703
Jamming Attack	1343
Proposed System	100

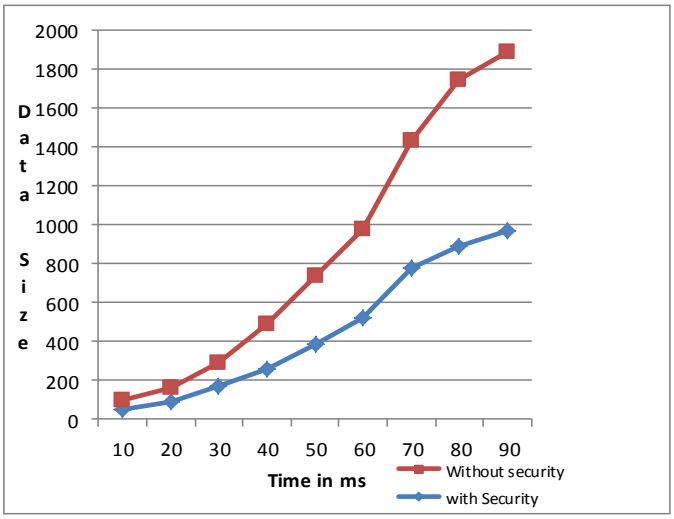

Fig3: Data Delivery Ratio

TABLE II DATA DELIVERY RATIO

Time in ms	Data size With security	Data size Without security
10	53	42
20	88	73
30	168	125
40	258	230
50	386	350
60	522	456
70	780	658

The aim of our system is to increase lifetime and security in the network, in the first graph we shows that how we increased lifetime and this graph shows the time required for sending the specific size of data with and without security, as we are providing the security the time should be more as compared to normal sending for security we are using the encryption algorithm for security.

V. CONCLUSIONS

In this paper we have performed a tradeoff analysis of energy consumption and QoS requirement to reliability gain and timeliness as well as to provide security for redundancy management of clustered heterogeneous wireless sensor networks by utilizing multipath routing to answer user queries. In our work, we consider redundancy management of multipath routes, based on trust and energy values, for intrusion detection, and to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes. we have noted that increasing source redundancy as well as path redundancy will enhances the reliability and security. However, it also decreases the energy consumption and thus it contributing to the increase of the system lifetime.

ACKNOWLEDGMENT

I have great pleasure and satisfaction in presenting this paper on "Redundancy Management of Multipath Routing for Intrusion Tolerance of Packet Loss by Malicious Node in HWSN". I take this opportunity to express my sincere thanks to all those people who have helped me to complete this paper successfully. \\

I would like to express my immense gratitude to my guide Prof. N. R. Wankhade for his helpful attitude, patience, contacts and moral support and encouragement throughout this work. He has been always there providing sufficient support with his excellent expertise in this area.

REFERENCES

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL*. 10, NO. 2, JUNE 2013.

[2] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput*., vol. 3, no. 4, pp. 366–379, 2004.

[3] E. Felemban, L. et al, "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.

[4] I. R. Chen, et.al, "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.

[5] 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

[6] 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.

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

[8] 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

[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.

[10] 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.

[11] 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 Net*.

[12] Y. Zhou, Y. Fang, et.al., "Securing wireless sensor networks: a survey*," IEEE Commun. Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[13] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," J. Netw. Comput. Appl., vol. 33, no. 4, pp. 422–432, 2010.

[14] J. Deng, et. al, "INSENS: intrusion-tolerant routing for wireless sensor networks," Computer Commun., vol. 29, no. 2, pp. 216–230, 2006

[15] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in Proc. 2006

[16] 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

