Model Based Analysis for QoS Guarantee by Intrusion Detection System in Heterogeneous Wireless Sensor Networks

S.N. Anusha[1], G.Thavaseelan[2],
PG Scholar[1], Assistant Professor[2],
St.Peter's University, TN, India

Abstract – In this paper we propose a model based analysis to provide QoS Guarantee by using the Intrusion Detection System(IDS) in Heterogeneous wireless sensor networks(HWSN).The key concept of our model based analysis is to provide a multipath routing with redundancy management in which the query response probability is maximized and to increase the lifetime of network. In HWSN a voting based intrusion detection algorithm is used to overcome the trade-off problem between energy consumption vs gain in QoS parameters. The Maximization of lifetime of network is achieved by using the dynamic redundancy algorithm which is used in fault tolerant control.

Keywords- Redundancy management, Intrusion Detection System, QoS parameters.

I. INTRODUCTION

The objective of dynamic redundancy management is to dynamically identify and apply the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters to maximize Mean time to Failure (MTTF), in response it tends to environment changes of source/cluster head node density, radio range and capture rate. Numerous wireless sensor networks (WSN) are deployed in an unsupervised environment in which the energy replenishment is very difficult to maintain. Due to lack of resources the WSN cannot fulfill the QoS requirements such as reliability, timeliness and security and it also satisfy the energy consumption to increase the lifetime of HWSN. The "Clustering" is used to satisfy the above requirements. A cluster combines the resources of two (or) more computing devices together. Clustering improves the system's availability to user and aggregates to overall tolerance to fault, component failures. Our study explains the performance of heterogeneous WSN is much more better than the homogeneous WSN. The presence of malicious nodes in the path will break the path so that the trade-off between energy consumption vs QoS gain will get more complicated in both homogenous and heterogeneous WSN. In particular heterogeneous WSN the Cluster heads (CH) may get affected in the data delivery. In this case we use Intrusion Detection System (IDS),which is used to detect and evict the presence of malicious nodes. The model based analysis which is represented as a single term but it defines the redundancy management and the type of routing which is used.

ICGPC 2014
St.Peter's University, TN, India.

In this paper we use the multipath routing which is a best method of routing in this the fault tolerance and data delivery is much improved. Even though the multipath routing is tolerant of fault but by the recent studies tells that the trade-off issue will reduce the lifetime of the WSN. In the presence of unreliable and malicious nodes the redundancy is routed through a sink node, this is considered to maximize the lifetime of network and is attained by query success probability. This is considered as optimization problem and the voting based intrusion detection algorithm which is used to remove the unreliable nodes.

In this paper the model based analysis is introduced in which the multipath redundancy level and intrusion detection setting are used to satisfy the QoS requirements and to maximize the lifetime of the HWSN. For the intrusion tolerance we consider the problem in which the "selection of paths" and the "number of paths" are considered in which the "selection of paths" is solved by using light weighted IDS are used. For "numbers of paths" the paths are chosen depends in which the lifetime of the network is to be maximized. The paper is aligned as follows: In the section II, we discuss the related work which is contrast to our paper and about the existing work carried before. In the section III, we discuss the algorithm which is used in this paper. In the section IV the probability model (i.e.) the expressions in which the capture rate, query rate, reliability and energy consumption are given. In the section V, we discuss the conclusion and future enhancement of this paper.

II. LITERATURE SURVEY

Over the past few years, the numbers of protocols are used to find the trade-off problem between energy consumption, reliability and for secure communication. In the context [7] the routing operations and secure solution are provided. The MRR (multipath reliable routing) algorithm used to find reliable paths. In the context [3] the low cost sensors using wireless communication (i.e.) the WSN which is used for civil and military scenarios. Relative to [4], the detection of malicious nodes and unreliable nodes is performed and it is isolated. MDMP, a flat network provides immunity from various attack to improve network performance. In [12] the mechanism which is used to prevent WSN from attacks in an unprotected environment, the intrusion detection is used and it depends upon the restrictions and demands of the network. In the context [9] the QoS parameters such as timeliness and reliability are to be performed the difference between timeliness and reliability which improves the capacity of WSN. Relative to [1] our work propose a light weighted IDS

which has the characteristics of monitoring the neighborhood nodes to bring back to its normal operation. Relative to [16] Our work develops a adaptive fault tolerant QoS control algorithm in which the QoS requirements are satisfied which prolongs the lifetime of the network. The light weighted IDS which is used for monitoring, if anyone of the node is malicious then it may affect the others. Relative to [2] the intrusion detection in both ad-hoc network and WSN is used for security concern. Generally our paper has two approaches; one is usage of IDS which is mainly used for energy conservation so that the lifetime of network is maximized. The approach is MRR, a flat network which is used for feedback maliciousness and it can be used to route packets and to avoid maliciousness in the nodes. We provide a solution the trade-off problem between the energy consumption vs QoS gain, reliability and timeliness. Our paper provides a distinct concept from the existing work and in which voting based IDS is used in HWSN in which the redundancy is managed through the multipath routing and it provides the QoS guarantee. Our work also includes the parameters such as "source" and "path" redundancy which is used for lifetime maximization. A host based IDS monitors all or parts of the dynamic behavior and the state of a computer system. Besides such activities like dynamically inspect network k packets targeted at this specific host for energy conservation, we employ a distributed light-weight IDS by which intrusion detection is performed only locally.

III. SYSTEM MODEL

The HWSN mainly consists of sensors which have different capabilities. we are considering CH and SN, CH denotes the cluster head and SN denotes sensor nodes. The cluster head which is high in capabilities such as radio range, density and capture rate. The CH and SN are deployed in an unsupervised environment and it is distributed in homogeneous spatial. The λ_{CH} and λ_{SN} are the intensities of poisson processes respectively $\lambda_{CH} < \lambda_{SN}$. The transmission power and radio range are dynamically distributed so that the lifetime of the system. The radio range used by SN and CH is denoted by Υ_{CH} and Υ_{SN}. The transmission is done in multi hop routing without any acknowledgement and retransmission. It performs two conserving attacks they are bad-mouthing attacks and packet dropping attacks. Due to environmental conditions causes node failure which includes hardware failure and transmission failure. The hardware failure is denoted as 'q' and transmission failure is denoted as 'e'. The timeliness requirement is considered as Treq, the Treq should be delivered in a seconds or else the query fails. The timeliness is used in many emergency or military applications. The Model based analysis consists of redundancy management in multipath routing and it mainly consists of two types of redundancies, one is path redundancy and the other is source redundancy. one is path redundancy and the other is source redundancy. The path redundancy is denoted as (mp) and the source redundancy is denoted as (ms).The concept of clustering is introduced and a group of sensors which will form a cluster. The node is chosen depends upon the performance and the efficient node is taken as CH.

We use a pair-wise key established protocol in HWSN for security. Thus the SN with CH will form a cluster and the CH creates the pair-wise key with another CH. This prevents the system from malicious attacks.

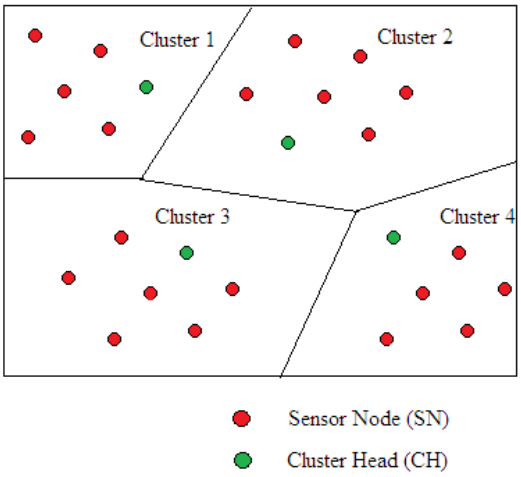

Fig.1.Redundancy management in HWSN

The host IDS (i.e.) light-weighted IDS is used for energy conservation and it do not have feedback mechanism such as MDMP. The neighbor node will continuously monitor the other nodes, the noise or error occurred is modeled by "host" false positive probability (Hpfp) and "host" false negative probability (Hpfn).The voting based distributed IDS which is used for removing the malicious nodes. The node 'm' is chosen randomly to collect the votes from the neighbor nodes and the votes are shared in secure transmission by usage of pair-wise keys. There is false positive probability(pfp) in which the nodes can identify incorrectly, good node as bad node and the false negative probability(pnp) which can misidentify bad node as good node and they are derived in the bad mouthing attacks.Mean time to failure (MTTF) which is used to translate the lifetime span of the actual system. The main objective of our paper is to find the best redundancy levels and the settings of IDS so that MTTF is maximized.

IV. PROBABILITY MODEL

In the section IV we develop a probability model, for the estimation of MTTF in HWSN for answering user queries by the usage of multipath data forwarding. We consider path redundancy (mp) and source redundancy (ms), we use the term (pfp) and (pnp) for both CH and SN but for differentiating CH and SN we define Pfp(CH) and Pnp(CH) for CH and for SN Pfp(SN) and Pnp(SN). The TIDS is the term which represents the intrusion detection interval parameters are identified to maximize the lifetime of the network. The above derived parameters are input parameters and the output parameter is denoted as MTTF. The radio range for CH and SN is denoted as Υ_{CH} and Υ_{SN} and the node density is represented as $\lambda(t)$ decreases due to the node failure. The reason of MTTF formulation is to estimate the number of queries and it is represented as Nq , since the system evolves dynamically the energy exhaustion changes dynamically.

The arrival rate is denoted as λq and the average of arrival rate is denoted as 1/ λq. The energy exhaustion due to query processing and intrusion detection for query *j* based on query arrival time Rq(tQ,j). The MTTF is computed by:

$$MTTF=\sum_{i=1}^{Nq-1} i \left(\prod_{j=1}^{i} R_q(t_{Q,j})\right)\left(1 - R_q(t_{Q,i+1})\right) + N_q \prod_{j=1}^{N_q} R_q\,(t_{Q,j}\,) \quad (1)$$

A. Network Dynamics:

When deployment all the nodes are considered as good nodes. The capture time of nodes are assumed as *fc(t)*. The probability of nodes is considered as *t* and for good node at time *t-TIDS* and it is denoted as *Pc* and it is given as:

$$\begin{aligned} Pc &= 1- P\{X > t, X > t - T_{IDS}\} \\ &= 1- \frac{P\{X > t, X > t - T_{IDS}\}}{P\{X > t - T_{IDS}\}} \\ &= 1- \frac{1-F_c(t)}{1-F_c(t-T_{IDS})} \end{aligned} \quad (2)$$

Here we are recalling the voting based distributed IDS are executed with the interval of T_{IDS}. The population of good and bad nodes are estimated at time and it is represented as *t I,i-1* and it is given as follows:

ngood t(I,i) = ngood(t I,i-1) - ngood(t I,i-1)×Pc
ngood t(I,i) = ngood(t I,i-1) + ngood(t I,i-1)×Pc

B. Query Success Probability:

We are using two ways of data forwarding (a) transmission speed violation (b) sensor/channel failures. As in the context [11] The first source of failure, transmission speed violation, accounts for query deadline violation. To know the failure probability due to transmission speed violation, we first derive the minimum hop-by-hop transmission speed required to satisfy the query deadline. Let d_{SN-CH} be the *expected* distance between a SN (selected to report sensor readings) and its CH and d_{CH-PC} be the *expected* distance between the source CH and the PC accepting the query result. Given a query deadline *Treq* as input, a data packet from a SN through its CH to the PC must reach the PC within *Treq*. Thus, the minimum hop-by-hop transmission speed denoted by *Sreq* is given by:

$$Sreq = \frac{d_{SN\text{-}CH} + d_{CH\text{-}PC}}{T_{req}} \quad (3)$$

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. The source CH will fail to deliver data to the PC if one of the following happens: (a) none of the CHs in the first hop receives the message; (b) in the first hop, *i* ($1 \le i < mp$) CHs receive the message, and each of them attempts to form a path for data delivery; however, all *i* paths fail to deliver the message because the subsequent hops fail to receive the broadcast message; or (c) in the first hop, at least *mp* CHs receive the message from the source CH from which *mp* CHs are randomly selected to forward data, but all *mp* paths fail to deliver the message because the subsequent hops fail to receive the message.

C. Energy Consumption :

In this section we are going to estimate the amount of energy exhausted during a query interval, cluster interval and an IDS interval. It is also used for estimation of number of queries of system to handle before running the energy exhaustion. Let α be the ratio of IDS execution rate to query rate and β be the ratio of clustering rate to query arrival rate. The number of IDS cycles, clustering cycles before system's energy exhaustion is considered as αNq and βNq. The total energy consumed due to intrusion detection, clustering and query processing is equal to the system and it is represented as Nq and the equation is given as follows:

$$E_{init} = \sum_{i=1}^{\alpha N_q} E_{IDS}\left(t_{I,i}\right) + \sum_{i=1}^{\beta N_q} E_{clustering}\left(t_{c,i}\right) + \sum_{i=1}^{N_q} E_q(t_{Q,i}) \quad (4)$$

The energy spent in voting base IDS cycle is denoted as EIDS and it is given as follows :

$$\begin{aligned} E_{IDS}\left(t_{I,i}\right) &= E_{IDS}^{CH}\left(t_{I,i}\right) + E_{IDS}^{SN}(t_{I,i}) \\ E_{IDS}^{CH}\left(t_{I,i}\right) &= N_{CH}\left(t_{I,i-1}\right)[m(m-1)] \\ &[E_T^{CH} + n_{CH}\,(t_{I,i-1})E_R^{CH} \quad (5) \\ E_{IDS}^{SN}\left(t_{I,i}\right) &= N_{SN}\left(t_{I,i-1}\right)[m(m-1)] \\ &[E_T^{SN} + n_{SN}\,(t_{I,i-1})E_R^{SN} \end{aligned}$$

V. PERFORMANCE EVALUATION

Our process design which mainly consists of 200 sensor nodes each nodes which mainly have parameters such as radio range, capture rate and density. The concept of clustering is used and a group of sensor nodes is to form a cluster. Depends upon the range of above parameters the CH is to be chosen. Except the CH the rest of nodes are considered as Cluster member or Sensor nodes. For example if CH is denoted as CH[20] the sensor nodes in that cluster is denoted as j[20]. The design of the process is given below:

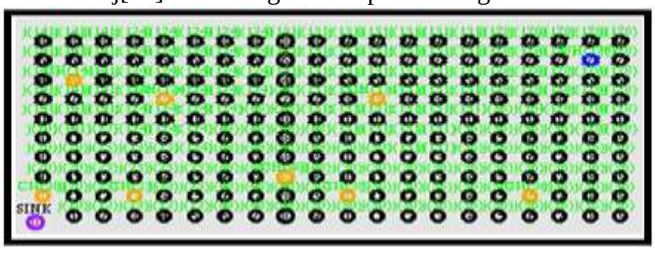

Fig 2. Design of sensor nodes with its CH

The Fig 2 shows the process design diagram in which the CH and the sensor nodes are shown in different colors and it is represented very clearly. After the execution of CH and the performance of the parameters such as query reliability, MTTF, good-put and the energy consumption is to be measured. The fig.3 below shows the effect of MTTF with respect to time.

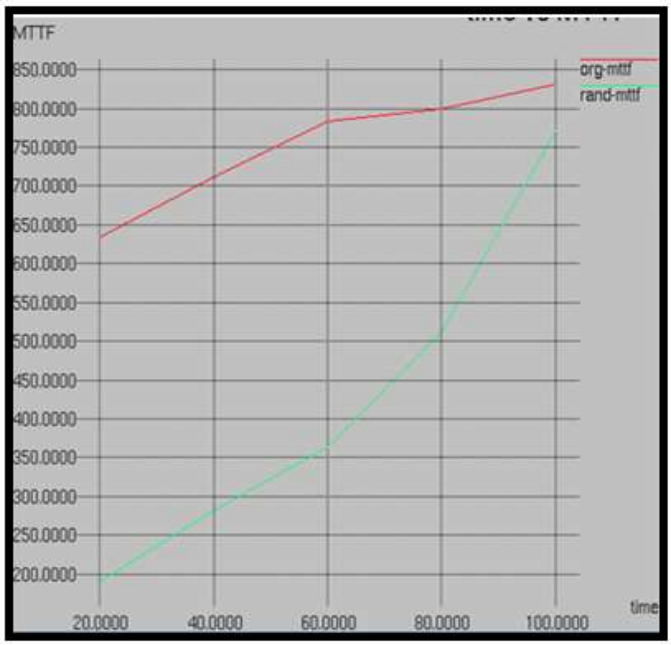

Fig.3 Effect of MTTF with respect to time

The figure [4] shows the energy consumed with respect to time and the energy consumption is much more reduced when compared to existing system.The Fig.5 shows the effect of query reliability with respect to the capture rate(packet/sec) and the performance is to be measured. When the capture rate is low, the population of malicious nodes is low. The fig.6 shows the performance evaluation of energy consumption which is much more reduced in our proposed paper. The main aim of our paper is to provide best redundancy level and to reduce the energy consumption by increasing the lifetime of the network using the IDS.

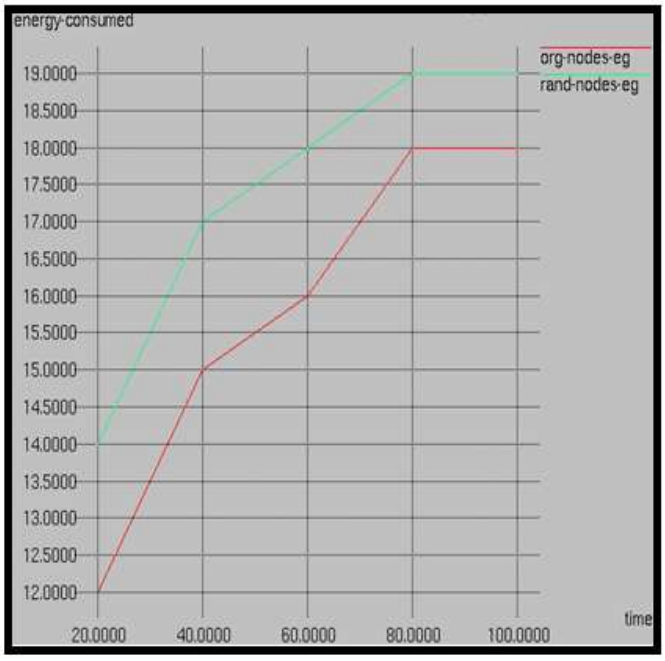

Fig.4 Energy consumed vs time

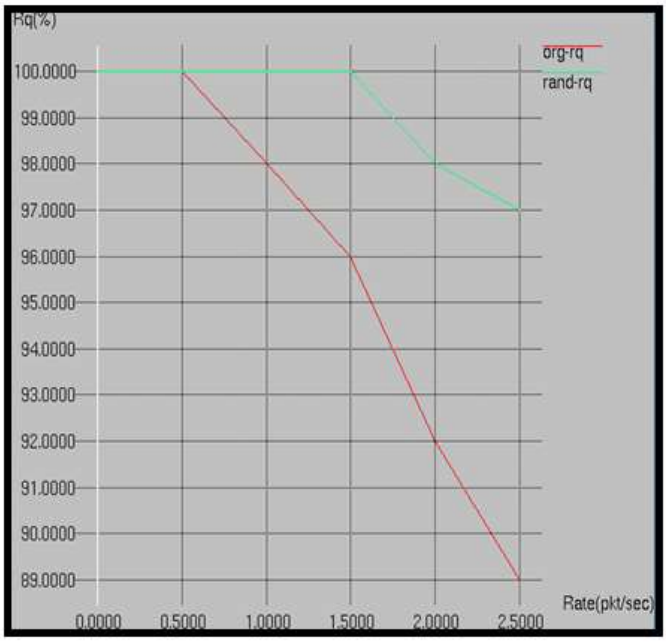

Fig.5 Effect of (mp,ms) with respect to capture rate

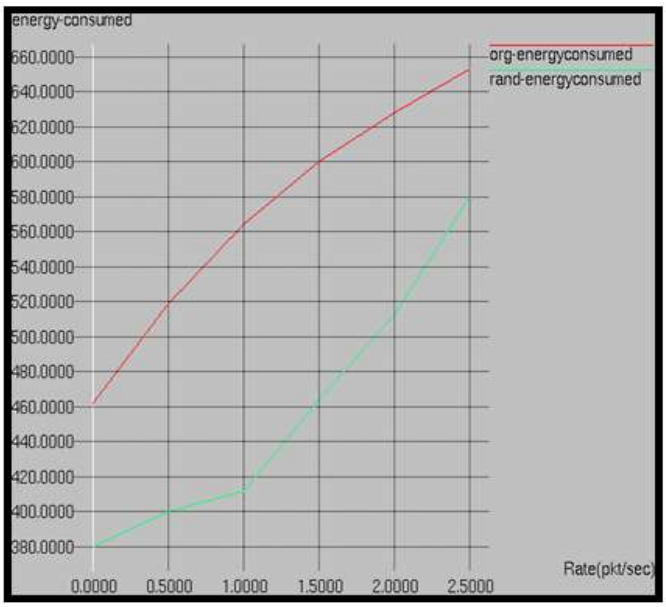

Fig. 6 Energy consumption vs capture rate

VI. CONCLUSIONS

In this paper we performed model based analysis which had explained the concept of redundancy management by utilizing multipath routing to answer the user queries. The method of IDS is used to identify and evict the attack of malicious nodes. The dynamic redundancy management algorithm is used to identify the best parameter setting so that the lifetime of the system is to be maximized.

For Future enhancement we plan to find more malicious attacks and in addition the packet dropping and bad mouthing attacks with different implementations to security, energy and reliability. Another method of "weighted voting" which is used to know the knowledge of neighbor nodes. For applications we use trust-based admission control scheme is used when the query traffic is heavy.

REFERENCES

[1] C. Haowen and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," in *Proc. 2005 IEEE Conf. ComputerCommun.*, pp. 524–535.

[2] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no.4, pp. 34–40, 2008.

[3] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008. 49–55.

[4] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection," in *Proc. 2009 Chinese ControlDecision Conf.*, pp. 4323–4328.

[5] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. 2007 European WirelessConf.*

[6] 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.

[7] D. Somasundaram and R. Marimuthu, "A multipath reliable routing for detection and isolation of malicious nodes in MANET," in *Proc. 2008Int. Conf. Computing, Commun. Netw.*, pp. 1–8.2010.

[8] 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.

[9] 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.

[10] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Commun.*, vol. 29, no. 2, pp.216–230, 2006.

[11] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in *Proc. 2006 Cyber Security Conf. Inf.Assurance*.

[12] 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 SecurityWireless Mobile Netw.*

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

[14] H. Su and X. Zhang, "Network lifetime optimization for heterogeneous sensor networks with mixed communication modes," in *Proc. 2007 IEEEWireless Commun. Netw. Conf.*, pp. 3158–3163.

[15] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal power management scheme for heterogeneous wireless sensor networks: lifetime maximization under QoS and energy constraints," in *Proc. 2007 Int. Conf. Netw.Services*, pp.69-69.

[16] I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," *IEEE Trans. Dependable Secure Computing*, vol. 8, no. 2, pp. 161–176, 2011.

[17] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management," *IET Commun.*, vol. 4, no. 7, pp. 758–767, 2010.

[18] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs," *Comput. Netw.*, vol. 54, no. 13, pp. 2215–2238, 2010.

[19] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Programming Languages Syst.*, vol. 4, no. 3, pp. 382–401, 1982.