Management Redundancy of Multipath Routing for Intrusion Tolerance in HWSNs

[1]CHINTHAPATLA SOWMYA, [2]M.MOHANRAO

Department of CSE
Megha Institute of Engineering & Technology For women's
Edulabad, Ghatkesar mandal, RangaReddy Dist. Telangana, India

Abstract: **In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We develop a novel probability model to analyze 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 and the intrusion invocation interval under which the lifetime of a HWSN is maximized. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime**.

Keywords: **Heterogeneous wireless sensor networks; multipath routing; intrusion detection; reliability; security; energy conservation.**

I. INTRODUCTION

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 tradeoff 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 attackers. It is commonly believed in the research community that clustering is an effective solution for achieving scalability, energy conservation, and reliability. Using homogeneous nodes which rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED [2] for lifetime maximization has been considered [3, 4]. Recent studies [5-7] demonstrated that using heterogeneous nodes can further enhance performance and prolong the system lifetime.

In the latter case, 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 (HWSN) environments in which CH nodes may take a more critical role in gathering and routing sensing data. Thus, very likely the system would employ an intrusion detection system (IDS) with the goal to detect and remove malicious nodes. While the literature is abundant in intrusion detection techniques for WSNs [8-12], the issue of how often intrusion detection should be invoked for energy reasons in order to remove potentially malicious nodes so that the system lifetime is maximized (say to prevent a Byzantine failure) is largely unexplored. The issue is especially critical for energy constrained WSNs designed to stay alive for a long mission time. 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 [3, 4], some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

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 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. We consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. Our contribution is 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. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve: (1) how many paths to use and (2) what

paths to use. To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols (e.g., MDMP for WSNS or AODV for MANETs), nor the use of feedback information to solve the problem. Rather, for energy conservation, we employ a distributed light-weight IDS by which intrusion detection is performed only locally. Nodes that are identified compromised are removed from the HWSN. Only compromised nodes that survive detection have the chance to disturb routing. One main contribution of our paper is that we decide "how many paths to use" in order to tolerate residual compromised nodes that survive our IDS, so as to maximize the HWSN lifetime. The rest of the paper is organized as follows. In Section II we discuss Literature Review. In Section III, we define Research Methodology. In Section IV, we present a dynamic management algorithm for managing redundancy of multipath routing for intrusion tolerance to maximize the system lifetime while satisfying the system reliability, timeliness and security requirements in the presence of unreliable wireless communication and malicious nodes. Finally in Section V we conclude the paper and outline some future research areas.

II. LITERATURE REVIEW

Over the past few years, many protocols exploring the energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In, the optimal communicat-ion range and communication mode were derived to maximize the HWSN lifetime. In, the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a HWSN with CH nodes having larger energy and processing capabilities than normal SNs in the network. The solution is drawn as an optimization problem to balance energy consumption across all nodes within the network along with their roles. In either work, no consideration was taken in to the account about the existence of malicious nodes in the network. Relative to the proposed work considers heterogeneous nodes with different densities and capabilities. However, the work also considers the presence of malicious nodes and explores the tradeoff in energy consumption and QoS gain in both security and reliability to maximize the system lifetime. In the context of secure multipath routing for intrusion tolerance, in the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. In the authors considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs the research proposed work also uses multipath routing to tolerate intrusion. However, the work specifically focuses on the amount of energy being consumed for intrusion detection and also to reduced energy consumption in multipath routing to tolerate intrusion. Moreover, the work consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection so that the energy consumption is reduced considerably along with security and reliability gain to maximize the system lifetime. In, voting based IDS approach given the tradeoff between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime. In general there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach is applicable to flat WSNs where an intermediate node provides a feedback about the maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach the author adopt in to use local host-based IDS for energy conservation (with SNs monitoring neighbor SNs and CHs monitoring neighbor CHs only), coupled with voting to cope with node collusion for implementing IDS functions. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions.

The solution author considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime. Compared with existing works cited above, the proposed research work extends from with considerations given to explore more extensive malicious attacks, security and reliability, and also investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. In addition to this, the proposed work also consider smart and insidious attackers which can perform more targeted attacks, capture certain nodes with high probability, alternate between benign and malicious behavior and concatenate with other attackers to avoid intrusion detection also to investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes. Using weighted voting scheme in intrusion detection system (IDS) would considerably reduce the false positives (FPs) and false negatives (FNs) ratio. For effective fault tolerance ad hoc on-demand multipath distance vector (AOMDV) is used to achieve reliability and QoS gain with minimum energy consumption.

III. RESEARCH METHODOLOGY

In Cluster-Based WSN, due to the heterogeneous nature of SNs, the capability of CH is greater than general SN. Additionally, because CH aggregates sensed data from SNs, it therefore often suffers attack. The CH used to detect intruders, which not only reduces the consumption of energy, but also efficiently decrease the amount of information in the entire network. The Cluster-Based WSN has following features.

- Self-organization
- Short-range broadcasting communication and multipath routing
- Dense deployment of the sensors
- Frequently changing topology, due to fading and node failures
- Limitations in computational resources, such as battery power and memory

In the proposed research hierarchical trust management for trust-based intrusion detection architecture is consider through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes. Voting involves the derivation of an output data object from a collection of n input data objects, as prescribed by the requirements and constraints of a voting algorithm. In data fusion, voting is method of combining different data delivered by several sources (e.g. sensors) whose outputs may be mistaken, delayed, or completely missing. In high reliable systems, voting is required whether the multiple computation channels comprise redundant hardware units, different software modules, identical hardware and software with various data, or any other combination of hardware, program and/or data redundancy. The main aim of any voting algorithms is to achieve high dependable outputs out of redundant components in order to increase the level of the entire critical-system dependability. Considering this aim, the characteristic/behavior of voting algorithms and the concept associated with theory of each evaluation parameter is one of the proper ways to develop any voting algorithm design methodology. The proposed design approach based on a well understanding of the concept of dependability leads to considerably reduce the false positives (FPs) and false negatives (FNs) ratio. Voting algorithm is considered as a widely used fault masking strategy for increasing the dependability of real-time critical computer systems. The dependability of a voter can clearly affect the whole system performance. Consequently, quantifying the dependability aspects for the results of voting algorithm is a key issue in evaluation voting algorithms.

The proposed design makes use of on-demand multipath protocol called ad hoc on-demand multipath distance vector (AOMDV) specially developed for heterogeneous WSN. AOMDV is based on a prominent and well-studied on-demand single path protocol known as ad hoc on-demand distance vector (AODV). AOMDV extends the AODV protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths so computed are guaranteed to be loop-free and disjoint. AOMDV has three novel aspects compared to other on-demand multipath protocols. First, it does not have high inter-nodal coordination overheads like some other protocols (e.g., TORA, ROAM). Second, it ensures disjointness of alternate routes via distributed computation without the use of source routing. Finally, AOMDV computes alternate paths with minimal overhead, it does this by exploiting already available alternate path routing information as much as possible the research proposes an intrusion framework for information sharing, which utilizes hierarchical architecture to improve intrusion detection capability for all participating nodes. Following are the key concept for intrusion framework.

A. Local Agent

The local agent is responsible for monitoring the information transmitted and received by the sensor. The node maintains an internal database which stores information about malicious nodes in network. When the network is configured, the sensor nodes lack any knowledge about malicious nodes. The signature database is gradually constructed, after the deployment of WSNs. The entry into the malicious node database is created and propagated to every node by CHs.

B. Global Agent

The global agent is responsible for monitoring the communication of its neighbor nodes. Due to the broadcasting nature of wireless sensor networks, every node can receive all packets within its communication range. We use the monitoring mechanism and pre-defined routing rules with two-hop neighbor knowledge to monitor these packets. If the monitor nodes discover any potential breach of security in their radio range, they create and send an alert to the CHs. Then, the CHs on receiving the alert, makes the decision about a suspicious node accordingly. Both agents are implemented in the application layer.

C. Evaluation of Alert Packets

The CHs are responsible for alert aggregation and computation. The research proposes four levels of trust, so that it can compute the alert counter for each malicious node, based on trust states of our monitor nodes. The malicious counter defines the threshold value of malicious activities of a sensor node which cannot be exceeded. If the value of the malicious counter of a sensor node exceeds the threshold, the sensor node is revoked from the cluster and WSNs.

1. After deployment, the sensor node builds its direct neighbor node's list and sends it to the sink node.
2. The sink node finds the set of nodes which corporately cover all nodes in the network as the chosen monitor nodes.
3. The sink node sends the request message to these chosen nodes to require them activating their intrusion detection modules.
4. Every message sent by sensor node or sink node is authenticated by using their shared keys.

In this section, research works apply hierarchical trust management protocol for trust-based intrusion detection. The propose research first describes the algorithm that can be used by a high-level node such as a CH (or a base station) to perform trust-based intrusion detection of the SNs (or CHs respectively) under its control. Then, research work will develop a statistical method analyzing various parameters to assess trust based IDS false positive and false negative probabilities using weighted voting. Without loss of generality, how a CH performs trust-based intrusion detection on SNs in its cluster will be illustrate. In trust-based intrusion detection, various parameter will be analyze to prolong the lifetime of the network in terms of energy consumption and gain in QoS such as reliability, minimum delay and security.

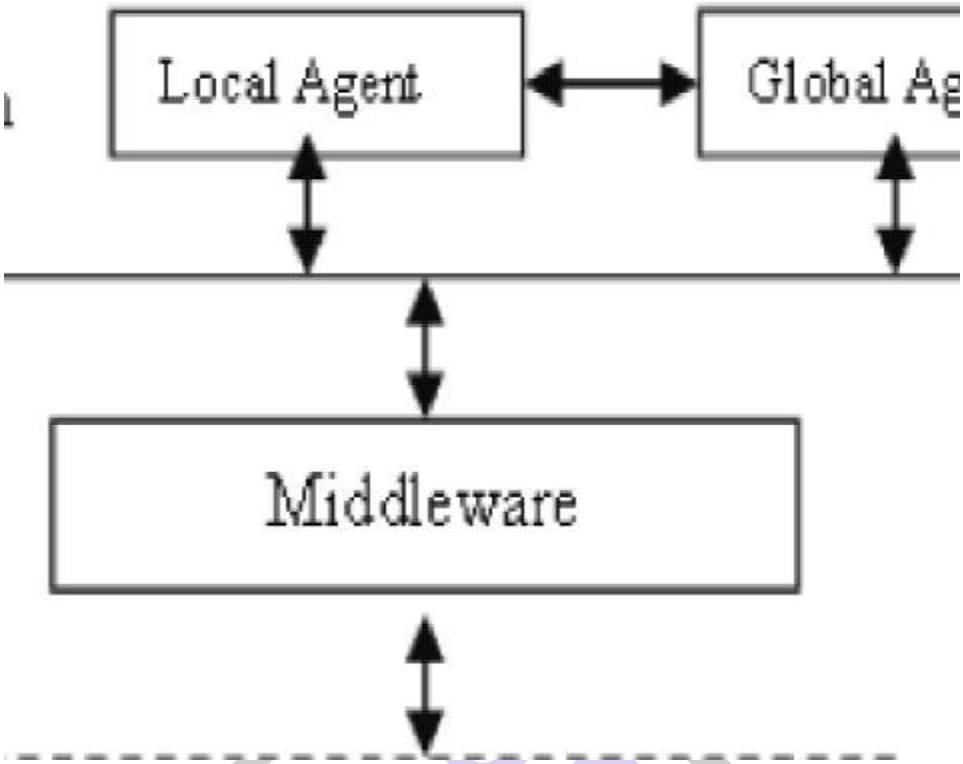

Fig.1. Hierarchical trust management for trust-based intrusion detection architecture

Due to battery depletion or hostile environments (e.g. wind, rain or high temperature) in which WSN may be deployed, sensor nodes are prone to failure. A part of the network can be disconnected and critical data maybe lost because of faults. Thus, fault tolerance is a major concern in wireless sensor networks and even more in critical applications such as healthcare, forest firefighting or nuclear radiation detection where it is not acceptable to lose sensitive data. Fault tolerance is the capacity to keep a network working correctly despite of failures. The Ad-hoc On Demand multipath Distance Vector (AOMDV) routing protocols balance the tradeoff between fault-tolerance and communication overhead. Indeed, increasing the number of paths for a better fault-tolerance. AOMDV is able to cope with route failure due to mobility. In particular, it reduces the packet loss by up to 40% and achieves a remarkable improvement in the end-to-end delay. AOMDV also reduces routing overhead by about 30% by reducing the frequency of route discovery operations, which in turn significantly increase the network resilience and lifetime.

IV. PERFORMANCE EVALUATION

In this section, we present numerical data obtained as a result of applying. Table I lists the set of input parameter values characterizing a clustered HWSN. Our example HWSN consists of 3000 SN nodes and 100 CH nodes, deployed in a square area of *A*2 (200m×200m). Nodes are distributed in the area following a Poisson process with density λSN =30 nodes/ (20×20 m2) and λCH =1 nodes/(20×20 m2) at deployment time. The radio ranges *rSN* and *rCH* are dynamically adjusted between 5m to 25m and 25m to 120m respectively to maintain network connectivity. The initial energy levels of SN and CH nodes are *E*0*SN* = 0.8 Joules and *E*0*CH* = 10 Joules so that they exhaust energy at about the same time. The energy parameters used by the radio module are adopted from [2]. The energy dissipation *Eelec* to run the transmitter and receiver circuitry is 50 nJ/bit. The energy used by the transmit amplifier to achieve an acceptable signal to noise ratio (*Eamp*) is 10 pJ/bit/m2 for transmitted distances less than the threshold distance *d*o (75m) and 0.0013 pJ/bit/m4 for distances greater than *d*o. The query arrival rate λq is a variable and is set to 1 query/sec to reveal points of interest. The query deadline ***Treq*** is strict and set to between 0.3 and 1 sec. The SN capture time is exponential distributed with rate λc such that $Pc = 1 - e\text{-}\lambda c \times TIDS$. We test the effect of λc by varying the inter-arrival time in between attacks (*Tcomp*) from 4 to 28 days, corresponding to an attack rate (λc) of once per 4 days to once per 28 days. The host IDS false positive probability and false negative probability (*Hpfp* and *Hpfn*) vary between 1% and 5% to reflect the host intrusion detection strength as in [11].

TABLE I: Input Parameter Values Characterizing A Query based Clustered HWSN

Parameter	Default Value
N_{SN}	3000
N_{CH}	100
λ_{SN}	30 nodes/(20 x 20 m^2)
λ_{CH}	1 node/(20 x 20 m^2)
E_0^{SN}	0.8 Joules
E_0^{CH}	10 Joules
r_{SN}	[5-25] m
r_{CH}	[25-120] m
$T_{clustering}$	60 sec
q	10^{-6}
e_f	[0.0001 – 0.1]
f	¼
λ_q	1 query/sec
T_{comp} (or $1/\lambda_c$)	[4-28] days
A	200m
n_b	50 bits
E_{elec}	50 nJ/bit
E_{amp}	10 pJ/bit/m^2
d_0	75m
T_{aq}	[0.3 – 1.0] sec
H_{pb}, H_{pb}	[0.01-0.05]

Fig.2 shows a high level description of the computational procedure to determine the optimal redundancy level (*mp*, *ms*) for maximizing MTTF. The MTTF is embedded on lines 15- 21 and 30-31 in Fig. 2. The accumulation of queries is shown on line 13. The value of *Nq* is computed on line 32. Lines 7 and 8 contain the conditions the system must hold to remain alive while computing an MTTF value for a specific redundancy level. The computational procedure essentially has a complexity of O (*mp* × *ms*) as it exhaustively searches for the best (*mp*, *ms*) pair, given a set of input parameter values as listed in Table I (above) as well as instance values of *m* (the number of voters for intrusion detection) and *TIDS* (the intrusion detection interval) characterizing a HWSN.

Fig.2. Computational Procedure to Determine Optimal (*mp, ms*) for Maximizing MTTF.

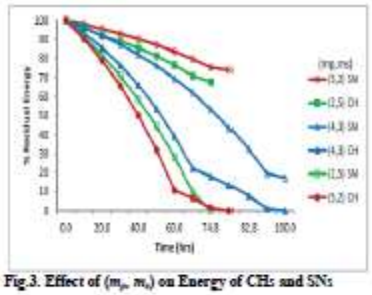

Fig.3. Effect of (m_p, m_s) on Energy of CHs and SNs

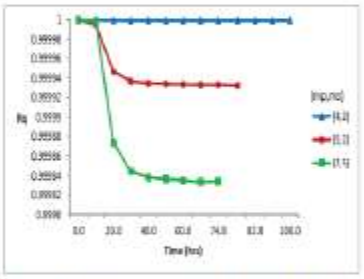

Fig.4. Effect of (m_p, m_s) on Query Reliability (R_q)

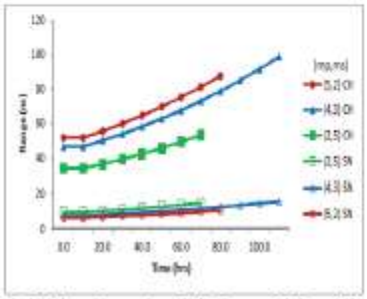

Fig.5. Effect of (m_p, m_s) on Radio Range of CHs and SNs

Below we present numerical data to provide evidence of the correctness of our analysis and to provide physical interpretations of the results. A query response propagates over SNs for source redundancy (*ms*) and over CHs for path redundancy (*mp*). Hence, *ms* directly affects energy consumption of SNs and *mp* directly affects energy consumption of CHs. Figs.3-5 summarize the effect of (*mp, ms*) on the CH/SN energy, query reliability, and CH/SN radio range, respectively, for the case in which *Tcomp* = 4 days and *TIDS* = 10 hrs. In Fig.3, a relatively high *mp* leads to quick energy depletion of a CH node. Similarly, a relatively high *ms* leads to quick energy depletion of a SN. While energy determines the number of queries the system is able to execute, the system lifetime largely depends on query reliability. Fig.4 shows the effect of (*mp, ms*) on query reliability. The combination of (4, 3) has the highest query reliability over other combinations of (2, 5) or (5, 2) in this test scenario. The system dynamically adjusts the radio range of CHs and SNs to maintain network connectivity based as nodes are being removed from the system because of failure or eviction. Fig.5 shows that the rate at which radio ranges of CHs and SNs increase are highly sensitive to *mp* and *ms*, respectively. A sharp increase of the radio range affects the energy consumption rate and thus the system lifetime. Overall, Figs. 3-5 indicate that there exist an optimal combination of (*mp, ms*) that will maximize the system lifetime. Fig.6 confirms that among three (*mp, ms*) combinations, (4, 3) results in the highest MTTF, since it has the highest query reliability without consuming too much energy per query execution.

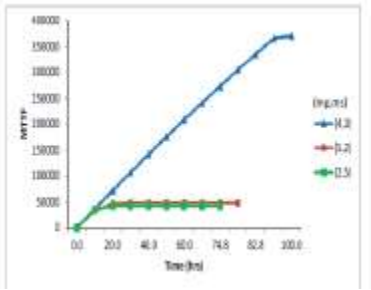

Fig.6. Effect of (*mp, ms*) on MTTF.

The correctness of our protocol design is evidenced by the effect of *Tcomp*, *m* and *TIDS* on optimal (*mp, ms*). Figs.7 and 8 show MTTF vs. (*mp, ms*) under low and high attack rates, respectively. First of all, in both graphs, we observe the existence of an optimal (*mp, ms*) value under which MTTF is maximized. Secondly, there exists an optimal *m* value (the number of voters) to maximize MTTF. In Fig. 8, *m*=7 yields a higher MTTF value than *m*=3 because in this scenario the attack rate is relatively high (one in four days), so a higher number of voters is needed to cope with and detect bad nodes more effectively, to result in a higher query success rate and thus a higher MTTF. Comparing these two graphs, we observe a trend that as the capture rate increases

(i.e., going from the left graph to the right graph), the optimal *m* value level increases. The reason is that as the capture rate increases, there are more and more malicious nodes in the system, so using more voters (e.g. *m*=7) can help identify and evict malicious nodes more effectively, thus increasing the query success probability and consequently the MTTF value. The system is better off this way to cope with increasing malicious node population for lifetime maximization even though more energy is consumed due to more voters being used. By comparing these two graphs, we observe a trend that as the capture rate increases (i.e., going from Fig.7 to Fig. 8), the optimal (*mp, ms*) redundancy level increases. When the capture rate increases from once in three weeks (*Tcomp* = 3 weeks) to once in four days (*Tcomp* = 4 days), the optimal *m* changes from *m*=3 to *m*=7. We also observe that the optimal (*mp, ms*) redundancy level changes from (3, 3) to (4, 4) when m=3. The reason behind this trend is that as more nodes are compromised in the system, a higher redundancy must be used to cope with packet dropping attacks. While increasing (*mp, ms*) consumes more energy, the gain towards increasing the query success probability (and thus towards increasing MTTF) outweighs the loss of lifetime due to energy consumption.

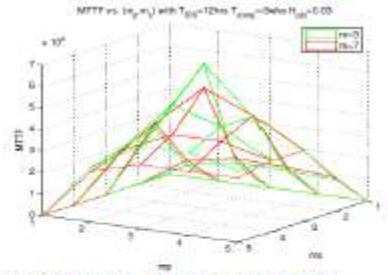

Fig.7. MTTF vs. (m_p, m_s) under Low Capture Rate.

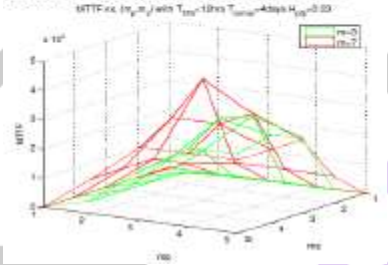

Fig. 8. MTTF vs. (*mp, ms*) under High Capture Rate.

Another trend exhibited in Figs.7 and 8 is that as the number of voters in intrusion detection (*m*) increases, the optimal (*mp, ms*) redundancy level decreases. This is because increasing *m* has the effect of detecting and evicting bad nodes more effectively, thus requiring a lower level of redundancy in (*mp, ms*) to cope with packet dropping attacks by bad nodes. In Fig.8, when *m*=3, the optimal (*mp, ms*) = (4, 4) while when *m*=7 the optimal (*mp, ms*) = (3, 3). In Fig. 9, we compare MTTF vs. (*mp, ms*) under three cases: (a) there are no malicious nodes and no intrusion detection, considering using multipath routing for fault tolerance only as in [8] (the top curve); (b) there are malicious nodes but there is no intrusion detection (the bottom curve); (c) there are malicious nodes and there is intrusion detection (the middle two curves). First of all, in each case we observe the existence of an optimal (*mp, ms*) value under which MTTF is maximized. Secondly, for the special case in which there are no malicious nodes (the top curve), the optimal (*mp, ms*) value to maximize MTTF is (3, 3) and the MTTF is the highest among three cases because there are no malicious nodes. When there are malicious nodes, however, the optimal (*mp, ms*) value becomes (5, 5) because using higher redundancy in multisource multipath routing is necessary to cope with malicious nodes that perform insider attacks. By applying intrusion detection, the MTTF value of the system under attack is increased. Fig.9 reflects the IDS case in Fig.7.

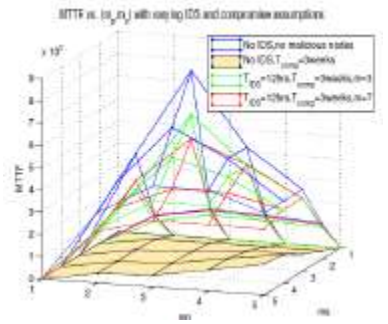

Fig. 9. MTTF vs. (*mp, ms*) for Three Cases.

We summarize the effect of *Tcomp* and *m* on the optimal (*mp, ms*) value in Table II and the effect of *Tcomp* on the optimal *m* value at which MTTF is maximized in Table III. Tables II shows that as the capture rate increases (i.e., a smaller *Tcomp*), the optimal (*mp, ms*) redundancy level should increase in order to cope with more bad nodes in the system performing packet dropping attacks. Also, as the number of voters (*m*) decreases and thus the detection strength decreases, the optimal (*mp, ms*) redundancy level should increase to cope with more bad nodes in the system. Table III shows that as the capture rate increases (i.e., a smaller *Tcomp*), the optimal *m* value level should increase so as to strengthen intrusion detection to remove more bad

nodes from the system. Also as *TIDS* decreases so that the detection strength increases, the optimal *m* value should decrease so as not to waste energy unnecessarily to adversely affect the system lifetime.

TABLE II: Optimal (*mp, ms*) With Varying *Tcomp* And *m*.

T_{comp}	m=3	m=5	m=7
4 days	(5,4)	(4,4)	(4,4)
1 week	(4,4)	(3,3)	(3,3)
2 weeks	(3,3)	(3,3)	(3,3)

TABLE III: Optimal *m* with Varying T_{comp} and T_{IDS}

T_{comp}	T_{IDS}=4hrs	8hrs	14hrs	18hrs	24hrs
4 days	3	5	7	7	7
1 week	3	5	5	7	7
2 weeks	3	3	5	5	7
3 weeks	3	3	5	5	5

We further ascertain the correctness of our analysis by the effect of *TIDS* (IDS detection interval) on MTTF. Figs. 10 and 11 show MTTF vs. *TIDS* with varying *m* under low capture rate (*Tcomp* = 3 weeks) and high capture rate (*Tcomp* = 1 week), respectively. We first observe that there exists an optimal *TIDS* value under which MTTF is maximized. Furthermore, the optimal *TIDS* value increases as *m* increases. For example, in Fig. 10 as *m* increases from 3, 5 to 7 we see that correspondingly the optimal *TIDS* at which MTTF is maximized increases from 8, 10 to 16 hours. The reason is that as the number of voter's increases so the intrusion detection capability increases per invocation, there is no need to invoke intrusion detection too often so as not to waste energy and adversely shorten the system lifetime. We also observe two general trends. One trend is that as *TIDS* increases, the optimal *m* value increases. The reason is that when *TIDS* is small so intrusion detection is invoked frequently, we don't need many voters per invocation so as not to waste energy unnecessarily to adversely shorten the system lifetime. The second trend shown in Figs. 10 and 11 is that as the node capture rate increases, the optimal *m* value increases in order to cope with more compromised nodes in the system. These two trends correlate well with those summarized in Table IV earlier.

TABLE IV: Optimal *TIDS* with Varying *Tcomp* and *m*

T_{comp}	m=3	m=5	m=7
4 days	6 hrs	10	14
1 week	8	10	16
2 weeks	14	24	36
3 weeks	24	40	52

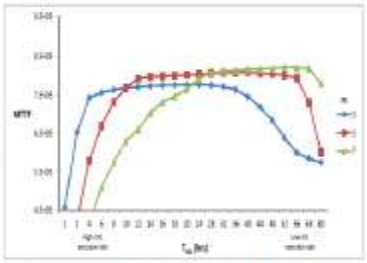

Fig 10. Effect of T_{IDS} on MTTF under Low Capture Rate

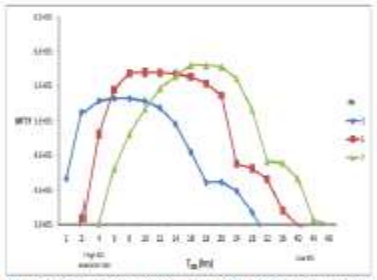

Fig 11. Effect of T_{IDS} on MTTF under High Capture Rate

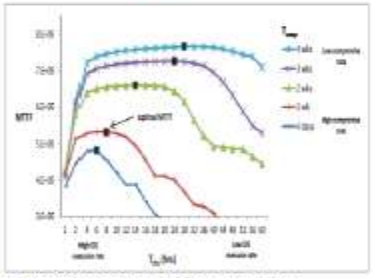

Fig 12. Effect of Capture Rate on Optimal T_{IDS}

TABLE V: Effect of Capture Rate on Maximum Radio Range To Maintain Connectivity

T_{comp}	r_{ss}	r_{cn}
4 days	21.5m	117.7m
1 week	15.9	82.2
2 weeks	11.4	62.4
3 weeks	10.9	60

Lastly, we examine the sensitivity of the optimal *TIDS* to the capture rate. Fig. 12 shows MTTF vs. *TIDS* with varying *Tcomp* values. It exhibits the trend that as the capture rate increases (a smaller *Tcomp* value), the optimal *TIDS* at which MTTF is maximized must decrease to cope with malicious attacks. For example, in Fig. 12 the optimal *TIDS* is 24 hours when *Tcomp* = 4 weeks and reduces to 6 hours when *Tcomp* = 4 days. The reason is that when the capture rate is low and hence the malicious node population is low, the negative effects of wasting energy for IDS execution (through evicting falsely identified nodes and executing the voting mechanism) outweighs the gain in the query success probability, so the system is better off by executing intrusion detection less often. On the other hand, when the capture rate is high and the malicious node population is high, the gain in the query success probability because of evicting malicious nodes often outweighs the energy wasted because of frequent IDS execution, so the system is better off by executing intrusion detection often. Table IV summarizes the effect of *Tcomp* and *m* on the optimal *TIDS* value at which MTTF is maximized. Table V further summarizes the effect of *Tcomp* on the maximum radio range required to maintain network connectivity in terms of the optimal redundancy level to prolong the system lifetime.

V. CONCLUSION

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 a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

For future work, we plan to explore more extensive malicious attacks in addition to packet dropping and bad mouthing 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. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection. Lastly, we plan to investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. In situations where concurrent query traffic is heavy, we plan to explore trust-based admission control to optimize application performance.

REFERENCES

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks", March 9, 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. 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.
[4] 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.
[5] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," 24th Annu. Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM), 2005, pp. 878-890 vol. 2.
[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," IEEE 61st Vehicular Technology Conference, 2005, 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., vol. 14, no. 5, pp. 56-63, 2007.
[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris, France, 2007.
[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. Rel., 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," 1st ACM Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.
[12] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6-28, 2008.