Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 84 (2015) 34083-34090

ISSN: 2229-712X

Adaptive Clustering in Multipath Routing for Intrusion Detection and Redundancy Management in Wireless Sensor Networks

K.Seena Naik and G.A.Ramachandra

Department of CST, S.K.University, Ananthapur, India.

ARTICLE INFO

Article history:

Received: 28 January 2015;

Received in revised form:

20 July 2015;

Accepted: 31 July 2015;

Keywords

Heterogeneous wireless sensor networks,

Multipath routing,

Intrusion detection;

Reliability,

Security,

Energy conservation.

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.

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 Manuscript received April 17, 2012; revised June 28, 2012 and January 30, 2013, accepted March 9, 2013. The associate editor coordinating the review of this paper and approving it for publication was C. Hong. Hamid Al-Hamadi and Ing-Ray Chen are with the Department of Computer Science, Virginia Tech, Falls Church, VA 22043; (e-mail: {hhamadi, irchen}@vt.edu).

(CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED [1] for lifetime maximization has been considered [2, 3]. Recent studies [4-6] 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 intrusion detection system (IDS) with the goal to detect and remove malicious nodes. While the literature is abundant in intrusion detection techniques for WSNs [7-11], 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 [12]) 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 [2, 3, 13], some attention has been paid to using multipath routing to tolerate insider attacks [14-16]. 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 distributedintrusion detection algorithm is applied to remove malicious

Tele:

E-mail addresses: seenasuna558@gmail.com

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 [17] or AODV for MANETs [18]), 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 related work and contrast our approach with existing work on multipath routing for intrusion tolerance and reliability enhancement. In Section III, we define our system model with system assumptions given. In Section IV we derive an analytical expression for the system lifetime, considering factors such as query rate, attacker behavior, node capture rate, link reliability, and energy consumption. In Section V we present numerical data and provide physical interpretations of the results. In Section VI, 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 VII we conclude the paper and outline some future research areas.

Related Work

Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [19], the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In [20], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs. The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes. In [21], the authors considered a two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime. Relative to [21] our work also considers heterogeneous nodes with different densities and capabilities. However, our work considers the presence of malicious nodes and explores the tradeoff between energy consumption vs. QoS gain in both security and reliability to maximize the system lifetime.

In the context of secure multipath routing for intrusion tolerance, [22] provides an excellent survey in this topic. In [15] 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 [14] the authors considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs. Our work also uses multipath routing to tolerate intrusion. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization. In [23] a randomized dispersive multipath routing protocol is proposed to avoid black holes. The randomized multipath routes are dispersive to avoid the black hole and to enhance the probability of at least k out of n shares based on coding theory can reach the receiver. The approach, however, does not consider intrusion detection to detect compromised nodes. Relative to [23] our work also uses multipath routing to circumvent black hole attacks for intrusion tolerance. Moreover, we consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection to best tradeoff energy consumption vs. security and reliability gain to maximize the system lifetime.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs. [7, 11] provide excellent surveys of the subject. In [10], a decentralized rule-based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The monitor nodes apply predefined rules to collect messages and raise alarms if the number of failures exceeds a threshold value. Our host IDS essentially follows this strategy, with the flaws of the host IDS characterized by a false positive probability (Hpfp) and a false negative probability (Hpfn). In [10], however, no consideration is given about bad-mouthing attacks by compromised monitor nodes themselves, so if a monitor node is malicious, it can quickly infect others. In [8], a collaborative approach is proposed for intrusion detection where the decision is based on a majority voting of monitoring nodes. Their work, however, does not consider energy consumption issues associated with a distributed IDS, nor the issue of maximizing the WSN lifetime while satisfying QoS requirements in security, reliability and timeliness. Our voting-based IDS approach extends from [9] with considerations given to 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 especially applicable to flat WSNs is for an intermediate node to feedback 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 [17, 24]. Another approach which we adopt in this paper is 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 (as discussed in III.11 and III.12 in the paper). Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions. Our solution 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, our work is distinct in that we consider redundancy management for both intrusion/fault tolerance through multipath routing and intrusion detection through voting-based IDS design to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes.

System Model

A HWSN comprises sensors of different capabilities. We consider two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources. We use and to denote the initial energy levels of CHs and SNs, respectively. While our approach can be applied to any shape of the operational area, for analytical tractability, we assume that the deployment area of the HWSN is of size A2. CHs and SNs are distributed in the operational area. To ensure coverage, we assume that CHs and SNs are deployed randomly and distributed according to homogeneousspatial Poisson $\lambda < \lambda$ with intensities and respectively, with processes used by CH and SN transmission. The radio ranges $\lambda\lambda$, transmission and, respectively. The radio range and the is denoted by power of both CHs and SNs are dynamically adjusted throughout the system lifetime to maintain the connectivity between CHs and between SNs. Any communication between two nodes with a distance greater than single hop radio range between them would require multi-hop routing. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission [2].

All sensors are subject to capture attacks, i.e., they are vulnerable to physical capture by the adversary after which their code is compromised and they become inside attackers. Since all sensors are randomly located in the operational area, the same capture rate applies to both CHs and SNs, and, as a result, the compromised nodes are also randomly distributed in the operation area. Due to limited resources, we assume that when a node is compromised, it only performs two most energy conserving attacks, namely, bad-mouthing attacks (recommending a good node as a bad node and a bad node as a good node) when serving as a recommender, and packet dropping attacks [25] when performing packet routing to disrupt the operation of the network..

Environment conditions which could cause a node to fail with a certain probability include hardware failure (q), and transmission failure due to noise and interference (e). Moreover, the hostility to the HWSN is characterized by a per-node capture rate of λc which can be determined based on historical data and knowledge about the target application environment. These probabilities are assumed to be constant and known at deployment time.

Queries can be issued by a mobile user (while moving) and can be issued anywhere in the HWSN through a nearby CH. A CH which takes a query to process is called a query processing center (PC). Many mission critical applications, e.g., emergency rescue and military battlefield, have a deadline requirement. We assume that each query has a strict timeliness requirement (Treq). The query must be delivered within Treq seconds; otherwise, the query fails.

Redundancy management of multipath routing for intrusion tolerance 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 PC through intermediate CHs. Fig. 1 shows a scenario with a source redundancy of 3 (ms = 3) and a path redundancy of 2 (mp = 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 [26]. Therefore, when the density is sufficiently high such that the average number of one-hop neighbors is sufficiently larger than mp and ms, we can effectively result in mp redundant paths for path redundancy and ms distinct paths from ms sensors for source redundancy.

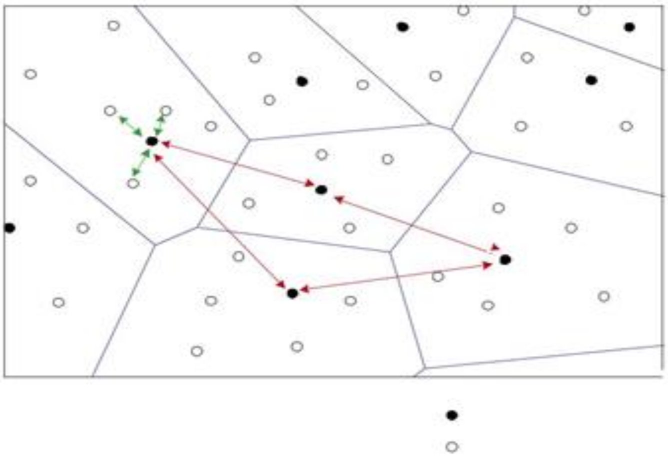

Fig 1. Source and Path redundancy for a Heterogeneous WSN

We assume that geographic routing [18], a well-known routing protocol for WSNs, is used to route the information between nodes; thus, no path information is maintained. The location of the destination node needs to be known to correctly forward a packet. As part of clustering, a CH knows the locations of SNs within its cluster, and vice versa. A CH also knows the location of neighbor CHs along the direction towards the processing center.

We assume that sensors operate in power saving mode (e.g. [27, 28]). Thus, a sensor is either active (transmitting or receiving) or in sleep mode. For the transmission and reception energy consumption of sensors, we adopt the energy model in [1] for both CHs and SNs.

To preserve confidentiality, we assume that the HWSN executes a pairwise key establishment protocol (e.g., [29, 30]) in a secure interval after deployment. Each node establishes pairwise keys with its k-hop neighbors, where k is large enough to cover a cluster area. Thus, when SNs join a new cluster, the CH node will have pairwise keys with the SNs joining its cluster. Since every SN shares a pairwise key with its CH, a SN can encrypt data sent to the CH for confidentiality and authentication purposes. Every CH also creates a pairwise key with every other CH. Thus a pairwise key exists for secure communication between CHs. This mechanism is useful to prevent outside attackers, not inside attackers.

To detect compromised nodes, every node runs a simple host IDS to assess its neighbors. Our host IDS is light-weight to conserve energy. It is also generic and does not rely on the feedback mechanism tied in with a specific routing protocol (e.g., MDMP for WSNS [17] or AODV for MANETs [18]). It is based on local monitoring. That is, each node monitors its neighbor nodes only. Each node uses a set of anomaly detection rules such as a high discrepancy in the sensor reading or recommendation has been experienced, a packet is not forwarded as requested, as well as interval, retransmission, repetition, and delay rules as in [10, 31-33]. If the count exceeds a system-defined threshold, a neighbor node that is being monitored is considered compromised. The imperfection of monitoring due to environment noise or channel error is modeled by a “host” false positive probability (Hpfp) and a “host” false negative probability (Hpfn) which are assumed known at deployment time.

To remove malicious nodes from the system, a voting-based distributed IDS is applied periodically in every time interval. A

CH is being assessed by its neighbor CHs, and a SN is being assessed by its neighbor SNs. In each interval, m neighbor nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node. The m voters share their votes through secure transmission using their pairwise keys. When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted. For both CHs and SNs, there is a system-level false positive probability that the voters can incorrectly identify a good node as a bad node. There is also a system-level false negative probability that the voters can incorrectly misidentify a bad node as a good node. These two system-level IDS probabilities will be derived based on the bad-mouthing attack model in the paper.

Here we note that increasing source or path redundancy enhances reliability and security. However, it also increases the energy consumption, thus contributing to the decrease of the system lifetime. Thus, there is a tradeoff between reliability/security gain vs. energy consumption. The distributed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily wasting energy so as to maximize the query success probability and the system lifetime. The effectiveness of the IDS depends on its parameters (and m). While a shorter or a higher m can result in low and , it also consumes more energy from the sensor nodes. Thus, this is another design tradeoff.

To provide a unifying metric that considers the above two design tradeoffs, we define the total number of queries the system can answer correctly until it fails as the lifetime or the mean time to failure (MTTF) of the system, which can be translated into the actual system lifetime span given the query arrival rate. A failure occurs when no response is received before the query deadline. The cause could be due to energy exhaustion, packet dropping by malicious nodes, channel/node failure, or insufficient transmission speed to meet the timeliness requirement. Our aim is to find both the optimal redundancy levels and IDS settings under which the MTTF is maximized, when given a set of parameters characterizing the operational and environment conditions.

Probability Model

In this section we develop a probability model to estimate the MTTF of a HWSN using multipath data forwarding to answer queries issued from a mobile user roaming in the HWSN area. Table I provides the notation used for symbols and their physical meanings. We use the same notation for both from a SN is and. When differentiating a CH

CHs and SNs, e.g.,

necessary, we use the superscripts or subscripts “CH” and “SN”, e.g., and for a CH, and is labeled as input, derived, design or for a SN. A parameter output. In particular, mp (path redundancy), ms (source redundancy), m (the number of voters for intrusion detection) And (the intrusion detection interval) are design parameters whose values are to be identified to maximize MTTF, when given a set of input parameter values charactering the operational and environmental conditions. Derived parameters are those deriving from input parameters. There is only one output parameter, namely, MTTF. Note that most derived parameters are dynamic, i.e., as a function of time. For example, node density denoted by λ(t) decreases over time because of node failure/eviction as time progresses. On the other hand, the, radio ranges for CHs and SNs, denoted by and increase over time to maintain network connectivity.

The basic idea of our MTTF formulation is that we first deduce the maximum number of queries, Nq, the system can possible handle before running into energy exhaustion for the best case in which all queries are processed successfully. Because the system evolves dynamically, the amount of energy spent per query also varies dynamically. Given the query arrival rate λq as input, the average interval between query arrivals is 1/λq. So we can reasonably estimate the amount of energy spent due to query processing and intrusion detection for query j based on the query arrival time. Next we derive the corresponding query success probability, that is, the probability that the response to query j arriving at time, is delivered successfully to the PC before the query deadline expires. Finally, we compute MTTF as the probability-weighted average of the number of queries the system can handle without experiencing any deadline, transmission, or security failure. More specifically, the MTTF is computed by:

+,- !" , % &1 − ,)$ +
= * + / " , (1)
#$ #$ &1 − * #$
∏ #$

Here accounts for the probability of the system being able to successfully execute i consecutive queries but failing the i+1th query. The second term is for the best case in which all queries are processed successfully without experiencing any failure for which the system will have the longest lifetime span.

Network Dynamics

Initially at deployment time all nodes (CHs or SNs) are good nodes. Assume that the capture time of a SN follows a distribution function Fc(t) which can be determined based on historical data and knowledge about the target application environment. Then, the probability that a SN is compromised at time, t, given that it was a good node at time t- , denoted by 1 is given by:

PC = 1 − P{X > t | X > t − TIDS }
= 1 − P{X > t, X > t − TIDS } = 1 −
1− Fc (t) (2)
P{X > t − TIDS } − Fc (t − TIDS)

Th We note that is time dependent. For the special case in
= 1 − 2 . Recall
which the capture 1time is exponential distributed with rate λc,

positive probability at time t below. The explanation to the false negative probability is similar. A false positive results when the majority of the voters vote against the target node (which is a good node) as compromised. The first term in Eq. accounts for the case in which more than 1/2 of the voters selected from the target node’s neighbors are bad sensors who, as a result of performing bad-mouthing attacks, will always vote a good node as a bad node to break the functionality of the HWSN. Since more than 1/2 of the m voters vote no, the target node (which is a good node) is diagnosed as a bad node in this case, resulting in a false positive. Here the denominator is the total number of combinations to select m voters out of all neighbor nodes, and the numerator is the total number of combinations to select at least mmaj bad voters out of nbad nodes and the remaining good voters out of ngood nodes.

Fig. 4 shows a high level description of the computational procedure to determine the optimal redundancy level (m_p, m_s) for maximizing MTTF. The MTTF Eq. (Eq. (1)) is embedded on lines 15-21 and 30-31 in Fig. 4. The$_{/}$ accumulation of queries is shown on line 13. The value of 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(m_p × m_s) as it exhaustively searches for the best ($m_{p,}$ m_s) pair, given a set of input parameter values as listed in Table II (above) as well as instance values of *m* (the number of voters for intrusion detection) and (the intrusion detection interval) characterizing a HWSN.

λq	1 query/sec
1BO (or 1/λc)	[4-28] days
A	200m
n_b	50 bits
Eelec	50 nJ/bit
Eamp	10 pJ/bit/m^2
	75m
X	
Treq	[0.3 – 1.0] sec
Hpf , *Hpfn*	[0.01-0.05]

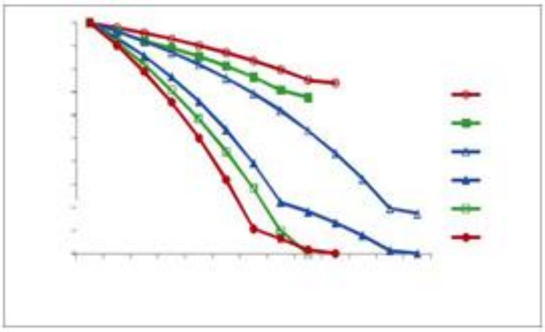

Fig 5. Effect of ($m_{p,}$ m_s) on Energy of CHs and SNs

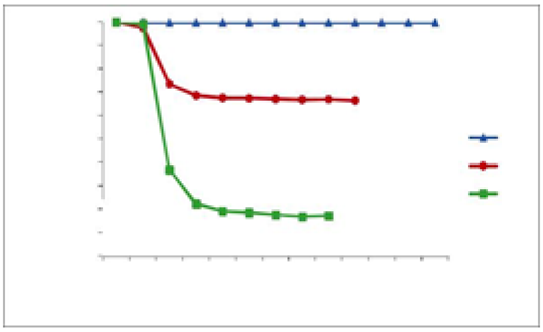

Fig. 6: Effect of ($m_{p,}$ m_s) on Query Reliability ( ).

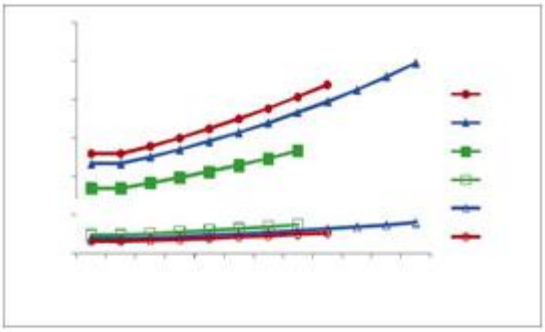

Fig 7. Effect of ($m_{p,}$ m_s) on Radio Range of CHs and SNs

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 (m_s) and over CHs for path redundancy (m_p). Hence, m_s directly affects energy consumption of SNs and m_p directly affects energy consumption of CHs. Figs. 5-7 summarize the effect of ($m_{p,}$ m) on the CH/SN energy, query reliability, and CH/SN radio range,^{s} respectively, for the case in which **1BO** = 4 days and = 10 hrs. In Fig. 5, a relatively high m_p leads to quick energy depletion of a CH node. Similarly, a relatively high m_s 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. 6 shows the effect of ($m_{p,}$ m_s) 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 on Eq. (10) as nodes are being removed from the system because of failure or eviction. Fig. 7 shows that the rates at which radio ranges of CHs and SNs increase are highly sensitive to m_p and m_s, respectively. A sharp increase of the radio range affects the energy consumption rate and thus the system lifetime. Overall, Figs. 5-7 indicate that there exist an optimal combination of ($m_{p,}$ m_s) that will maximize the system lifetime. Fig. 8 confirms that among three ($m_{p,}$ m_s) combinations, (4, 3) results in the highest MTTF, since it has the highest query reliability without consuming too much energy per query execution.

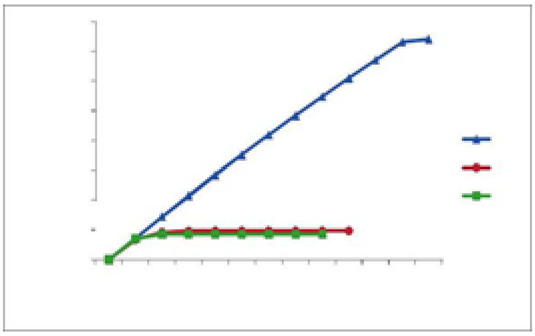

Fig 8. Effect of ($m_{p,}$ m_s) on MTTF

The correctness of our protocol design is evidenced by the effect of **1BO** , *m* and on optimal ($m_{p,}$ m_s). Figs. 9 and 10 show MTTF vs. ($m_{p,}$ m_s) under low and high attack rates, respectively. First of all, in both graphs, we observe the existence of an optimal ($m_{p,}$ m_s) value under which MTTF is maximized. Secondly, there exists an optimal *m* value (the number of voters) to maximize MTTF. In Fig. 10, *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. 9 to Fig. 10), the optimal ($m_{p,}$ m_s) redundancy level increases. When the capture **1BO** rate increases from once in three weeks (= 3 weeks) to once in four days (**1BO** = 4 days), the optimal *m* changes from *m*=3 to *m*=7. We also observe that the optimal ($m_{p,}$ m_s) 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 ($m_{p,}$ m_s) 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.

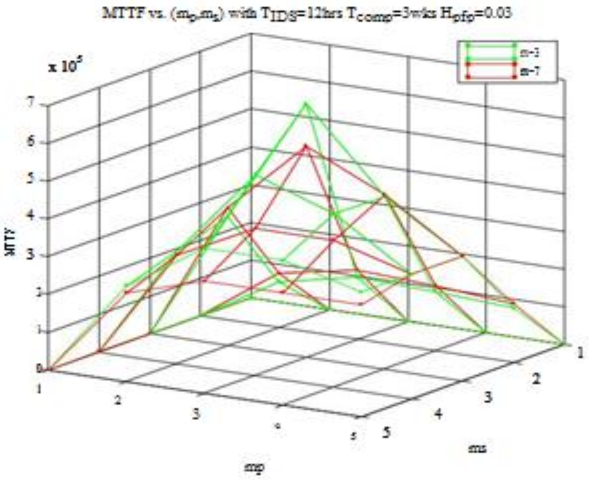

Fig 9. MTTF vs. ($m_{p,}$ m_s) under Low Capture Rate

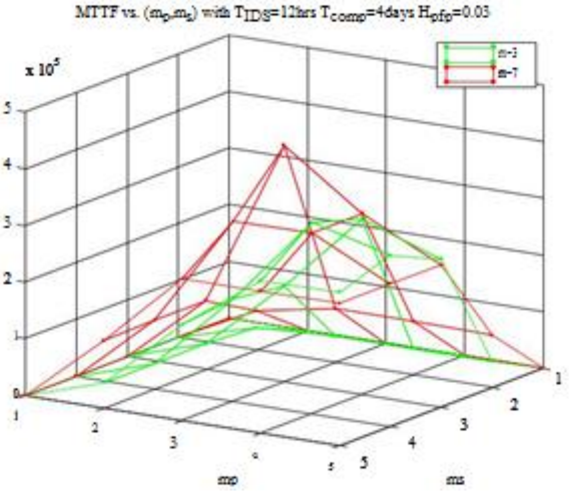

Fig 10. MTTF vs. ($m_{p,}$ m_s) under High Capture Rate.

Another trend exhibited in Figs. 9 and 10 is that as the number of voters in intrusion detection (*m*) increases, the optimal ($m_{p,}$ m_s) 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 ($m_{p,}$ m_s) to cope with packet dropping attacks by bad nodes. In Fig. 10, when *m*=3, the optimal ($m_{p,}$ m_s) = (4, 4) while when *m*=7 the optimal ($m_{p,}$ m_s) = (3, 3).

In Fig. 11, we compare MTTF vs. ($m_{p,}$ m_s) 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

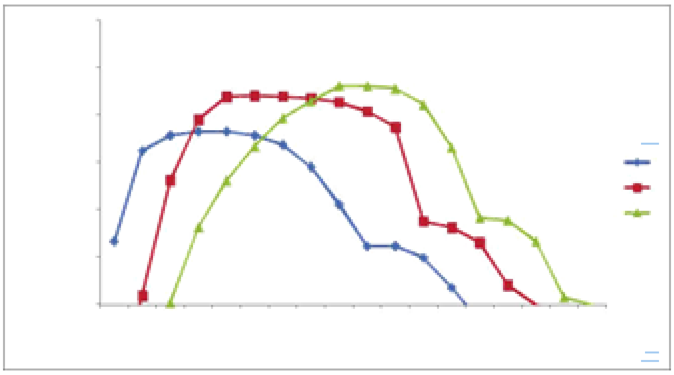

Fig 13. Effect of on MTTF under High Capture Rate

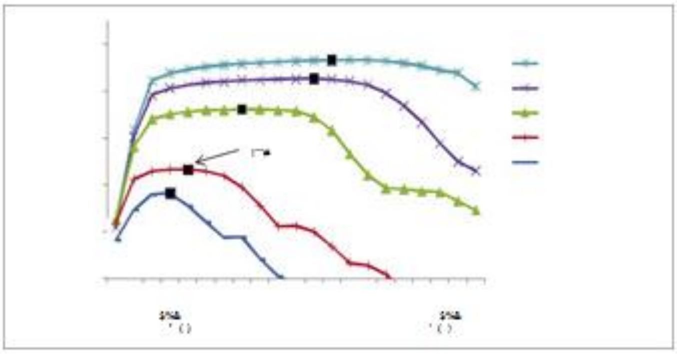

Fig 14. Effect of Capture Rate on Optimal TÎÏÐ

Table V: Optimal with varying 1bo and n.

‹•Ò¸	*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

Table VI: Effect Of Capture Rate On Maximum Radio ~~Range To Maintain Connectivity~~

‹•Ò¸	¦§	†‡
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 to the capture rate. Fig. 14 shows MTTF vs. with varying **1BO** values. It exhibits the trend that as the capture rate increases (a smaller **1BO** value), the optimal at which MTTF is maximized must decrease to cope with malicious attacks. For example, in Fig. 14 the optimal is 24 hours when **1BO** = 4 weeks and reduces to 6 hours when **1BO** = 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 V summarizes the effect of **1BO** and *m* on the optimal value at which MTTF is maximized. Table VI further summarizes the effect of **1BO** on the maximum radio range required to maintain network connectivity in terms of the optimal redundancy level to prolong the system lifetime.

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 (m_p) and source redundancy (m_s), as well as the best intrusion detection settings in terms of the number of voters (*m*) and the intrusion invocation interval ( ) 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 [33], [36], [37] 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 [38-40] to optimize application performance.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," IEEE 61st Vehicular Technology Conference, 2005, pp. 2528-2532.

[7] 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.

[8] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris, France, 2007.

[9] 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.

[10] 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.

[11] 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.

[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.

[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, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, 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," 9th Annu. Cyber Security Conf. on Information Assurance, Albany, NY, USA, 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.

[17] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection," Chinese Control and Decision Conference, 2009, pp. 4323-4328.

[18] D. Somasundaram and R. Marimuthu, "A Multipath Reliable Routing for detection and isolation of malicious nodes in MANET," International Conference on Computing, Communication and Networking, 2008, pp. 1-8.

[19] H. Su and X. Zhang, "Network Lifetime Optimization for Heterogeneous Sensor Networks With Mixed Communication Modes," IEEE Wireless Communications and Networking Conference, 2007, pp. 3158-3163.

[20] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal Power management scheme for Heterogeneous Wireless Sensor Networks: Lifetime Maximization under QoS and Energy Constraints," Third International Conference on Networking and Services (ICNS) 2007, pp. 69-69.

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

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

[23] T. Shu, M. Krunz, and S. Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941-954, 2010.

[24] Y. X. Jiang and B. H. Zhao, "A Secure Routing Protocol with Malicious Nodes Detecting and Diagnosing Mechanism for Wireless Sensor Networks," Asia-Pacific Service Computing Conference, The 2nd IEEE, 2007, pp. 49-55.

[25] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113-127.

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

[27] G. Bravos and A. G. Kanatas, "Energy consumption and trade-offs on wireless sensor networks," 16th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications 2005, pp. 1279-1283.

[28] S. Qun, "Power Management in Networked Sensor Radios A Network Energy Model," IEEE Sensors Applications Symp., 2007, pp. 1-5.

[29] C. Haowen and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," 24th Annu. Joint Conf. of the IEEE Computer and Communications Societies., 2005, pp. 524-535.

[30] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," 10th ACM conference on Computer and Communications Security, Washington D.C., USA, 2003.

[31] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," J. High Speed Netw., vol. 15, no. 1, pp. 33-51, 2006.

[32] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," IEEE Wireless Communications, vol. 15, no. 4, pp. 34-40, 2008.

[33] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 161-183, 2012.

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

[35] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660-670, 2002.

[36] C. J. Fung, Z. Jie, I. Aib, and R. Boutaba, "Dirichlet-Based Trust Management for Effective Collaborative Intrusion Detection Networks," IEEE Trans. Netw. Service Manag., vol. 8, no. 2, pp. 79-91, 2011.

[37] S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," Proceedings of the 4th international conference on Ubiquitous computing systems, Tokyo, Japan, 2007.

[38] I. R. Chen and T. H. Hsi, "Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers," Performance Evaluation, vol. 33, no. 2, pp. 89-112, 1998.

[39] S. T. Cheng, C. M. Chen, and I. R. Chen, "Dynamic quota-based admission control with sub-rating in multimedia servers," Multimedia systems, vol. 8, no. 2, pp. 83-91, 2000.

[40] S. T. Cheng, C. M. Chen, and I. R. Chen, "Performance evaluation of an admission control algorithm: dynamic threshold with negotiation," Performance Evaluation, vol. 52, no. 1, pp. 1-13, 2003.