IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. IV (Mar-Apr. 2014), PP 11-18
www.iosrjournals.org

Securing Multi-Path Routing Using Trust Management in Heterogeneous Wsn

B. Sathiyaprasad[1] , C.L.Stefi Sterlin[2]
[1] M.E Student, [2]Asst. Prof.,
Department of Computer Science and Engineering Sathyabama University Chennai-600119, India

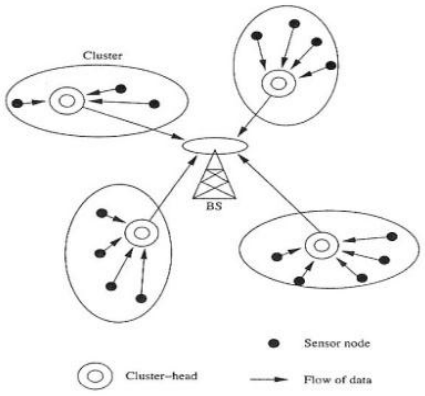
***Abstract**: In this paper we propose a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks. A highly scalable Cluster based trust Management Protocol is implemented to avoid malicious users in sensor nodes. This can be achieved by using Data Aggregation Protocol. The proposed protocol relies on a novel trust development algorithm (SELDA) is used by data aggregators and sensor nodes to select secure and reliable paths. The key concept of this paper is to maximize the system lifetime. Furthermore, a voting-based IDS algorithm is applied to detect malicious nodes in a heterogeneous wireless sensor network to analyze redundancy level in term of both source and path redundancy.*

***Index Terms:** Heterogeneous WSN, multipath routing, intrusion detection, reliability, security.*

I. Introduction

Wireless Sensor Networks consists of highly distributed networks of small, lightweight wireless nodes, deployed in large numbers and monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity. Formed by hundreds or thousands of nodes that communicate with each other and pass data along from one to another

- The sensor networks for each node consist of three subsystems:
  - Sensor subsystem: senses the environment
  - Processing subsystem: performs local computations on the sensed data
  - Communication subsystem: responsible for message exchange with neighboring sensor nodes
- Two important operations in a sensor networks
  - Data dissemination : the propagation of data/queries throughout the network
  - Data gathering : the collection of observed data from the individual sensor nodes to a sink.



II. Related Work

To improve Key Management in sensor networks, Sencun Zhu, Sanjeev Setia and Sushil Jajodia 2003 introduces a Key Management protocol for sensor networks to support an in network processing by establishing 4 keys for each sensor node. To prevent attacks in sensor networks, Chris Karlof and David Wagner 2003, developed a directed diffusion methods to avoid Sybil attack, sink hole attack, selective forwarding attack, acknowledgement spoofing attack. In Wireless Sensor Network mainly it focuses on energy consumption by using clustered sensor nodes. Here Ossama Younis and Sonia Fahmy 2004, planned to select the cluster head according to the hybrid energy of nodes and depending on the node degree. To maintain reliability and timeliness, Emad Felemban, Chang-Gun Lee and Eylem Ekici 2006, obtained a Multipath Multispeed routing protocol to deliver the packets to the destination node by using multiple paths.

To avoid spreading of compromised nodes in sensor networks, Jing Deng, Richard Han and Shivakant Mishra 2006 [5], introduced an algorithm called INSENS, it constructs forwarding table between each nodes to facilitate communication between sensor nodes and base station. In order to avoid insider attacks, Jin-Hee Cho, Ing-Ray Chen and Phu-Gui Feng 2010 [6], they produced an algorithm to avoid Byzantine failure and compromised nodes by means of Intrusion Detection.

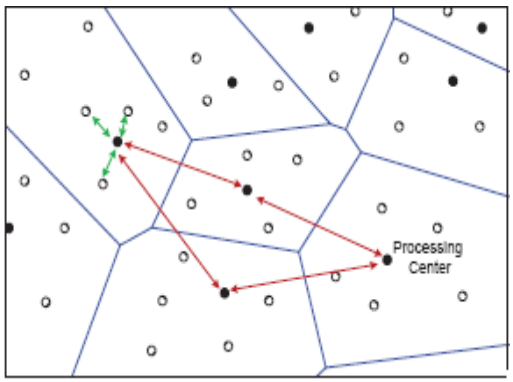


Fig (1) Source and Path Redundancy of heterogeneous WSNs

We consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection to best trade off energy consumption vs. security and reliability gain to maximize the system life time.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs, provide excellent surveys of the subject. In 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 (H_{pfp}) and a false negative probability (H_{pfn}).In 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 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 life time while satisfying QoS requirements in security, reliability and timeliness. Our voting-based IDS approach extends from with considerations given to the trade off between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime.

Energy efficiency is achieved by 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 life time of a HWSN in the presence of unreliable and malicious nodes.

III. System Model

We consider there are two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources. We use ECH init and ESN init 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 homogeneous spatial poisson processes with intensities λCH and λSN, respectively, with λCH<λSN. The radio ranges used by CH and SN transmission is denoted by rCH and rSN, respectively. The radio range and the transmission 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. 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 anode 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 are commender, and packet dropping attacks 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 any where 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 battle field, have a dead line requirement. We assume that each query has a strict timeliness requirement (T_{req}). The query must be delivered within T_{req} seconds; otherwise, the query fails. Redundancy management of intrusion tolerance for multipath routing is achieved through two forms of redundancy:(a) source redundancy by which m_s 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 m_p paths are used to relay packets from the source CH to the PC through intermediate CHs. Fig.1shows a scenario with a source redundancy of 3 (m_s =3) and a path redundancy of 2 (m_p =2). Therefore, when the density is sufficiently high such that the average number of one-hop neighbors is sufficiently m_s sensors for source redundancy. We assume larger than m_p and m_s, we can effectively result in m_p redundant paths for path redundancy and m_s distinct paths from that geographic routing, 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. 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 for both CHs and SNs. To preserve confidentiality, we assume that the HWSN executes a pair wise key establishment protocol in a secure interval after deployment. Each node establishes pair wise 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 pair wise keys with the SNs joining its cluster. Since every SN shares a pair wise key with its CH, a SN can encrypt data sent to the CH for confidentiality and authentication purposes. Every CH also creates a pair wise key with every other CH. Thus a pair wise key exists for secure communication between CHs. This mechanism is useful to prevent outside attackers, not inside attackers. 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 or AODV for MANETs). 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 rule. 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 (H_{pfp}) and a "host" false negative probability (H_{pfn}) which are assumed known at deployment time. To remove malicious nodes from the system, a voting-based distributed IDS is applied periodically in every TIDS 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 pair wise 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 P_{fp} that the voters can in correctly identify a good node as a bad node. There is also a system-level false negative probability P_{fn} 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 life time. Thus, there is a trade off between reliability/security gain vs. energy consumption. The distributed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily was ting energy so as to maximize the query success probability and the system life-time. The effectiveness of the IDS depends on its parameters (TIDS and m). While a shorter TIDS or a higher m can result in low P_{fp} and P_{fn}, it also consumes more energy from the sensor nodes. Thus, this is another design trade off.

To provide a unifying metric that considers the above two design trade offs, 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 life times pan 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.

ALGORITHM

Input: Data aggregator Aj , Aj 's neighboring nodes {N1;N2;…..Ni}reputation values {R1;j,R2;j ;….:Ri;j} of neighboring nodes with respect to Aj .

Output: Aggregated data Dagg.
Step 1: Aj observers each Ni periodically and updates the number of false and correct actions by Ni.
Step 2: Aj updates Ri,j value of each Ni based on the updated number of false and correct actions by Ni.
Step 3: Sensor nodes {N1; N2;...Ni} transmit data (D1;D2;…...;Di) to Aj .
Step 4: Aj weighs data Di of each sensor node Ni using the reputation value Ri,j.
Step 5: Aj aggregates the weighted data to obtain Dagg.

IV. Experemental Setup

a)Multi-Path Routing

Multipath Routing is the method of establishing multiple paths between given source to destination nodes within the network. The advantage for using multipath routing is

- Survivability
  - Provides redundancy.
- Congestion avoidance
  - Improves network utilization.
  - Provides load balancing.
- Management and control
  - Provides better performance in the presence of selfish or unregulated behavior.

In H-SPREAD they consider the multiple-to-one communication pattern of WSNs. HSPREAD protocol uses the threshold secret sharing scheme to split a message into N pieces, called shares. Each share is then forwarded by a source node to a different path towards the sink, where the original packet is reconstructed if at least T shares are received. H-SPREAD discovers multiple disjoint paths in two phases.

During phase one, the branch-aware flooding protocol is used to find a set of node-disjoint paths. Nodes tag their neighbors as a child, sibling or cousin, based on the branch that the node is located. Sensors found on a different tree branch form an alternative disjoint path. Phase one is achieved without the need to introduce any extra routing messages.

In phase two, authors use an extension of flooding in order to overcome the limitation of the branch-aware flooding that discovers extra paths at nodes that only have cousin neighbors.

b)Intrusion Tolerance

INSENS has the property that a single compromised node can only disrupt a localized section of the network and is not enough to stop the entire network from functioning.

c)Protocol Description

The basic INSENS protocol is divided into two parts: route discovery and data forwarding

1. Route discovery: route request

The route request message is flooded in the sensor network to inform each sensor node to send its neighbor-hood information to the base station. The base station initiates this first phase whenever it needs to construct the routing paths of all sensor nodes. The base station broadcasts a request message that is received by all its neighbors.

2.Route discovery: route feedback

After forwarding a request message in phase one, each sensor node waits for some fixed period of time before starting the second phase. In the second phase, a node unicasts a feedback message to the base station.

3. Route discovery: computing and propagating multipath routing tables

After sending its request message in the first phase, the base station waits for a certain period of time to collect all the connectivity information received via feedback messages. The base station constructs a topology of the network from these authenticated or verified feedback messages. Since some feedback messages may have been lost or dropped or tampered with the topology constructed by the base station may be incomplete.

4. Data forwarding

A node maintains a forwarding table that has several entries, one for each route to which the node belongs.

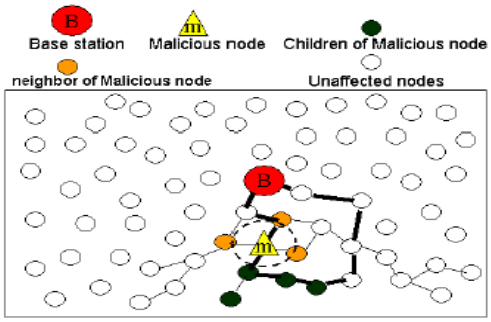


FIG (2) WSN topology rooted at the base station.

d)Secure and Reliable Data Aggregation

It reduces the effect of compromised nodes on aggregated data by using reputation values. Here the data of each sensor node is weighted based on its reputation value with respect to the data aggregator, by mitigating the effect of compromised nodes on the aggregated data. This can be achieved by using Reliable Data Aggregation (RDA).

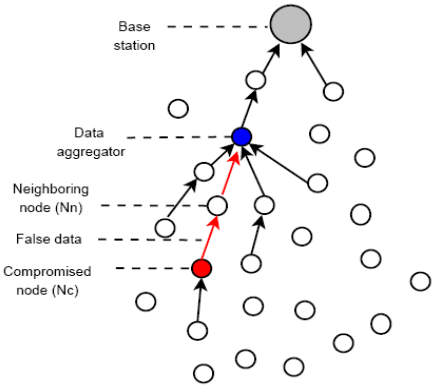


Fig: (3) Data forged by compromised node *Nc* is evaluated by neighboring node *Nn*'s high reputation value resulting in corrupted aggregated data.

e)Multipath Data Transmission To Dagg

In addition to data forgery, compromised nodes may also disrupt the network traffic by selectively forwarding or misdirecting packets. In order to prevent forgery and selective forwarding attacks by compromised nodes, we propose a secure multi path data transmission algorithm that ensures secure data delivery to data aggregators. The proposed data transmission algorithm secretly selects some paths based on the reliability of the paths and keeps the quantity and identity of the selected paths secret.

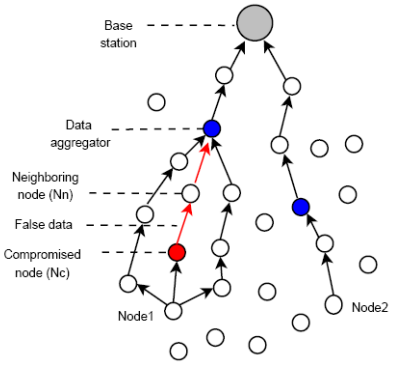


Fig (4) Multi path data transmission.

Node1 sends its data over multiple paths due to the compromised neighboring node. The data aggregator is able to detect the false data by comparing the multiple instances of the same data. On the other hand, Node2 uses only a single path to reach the data aggregator as it completely trusts its neighborhood.

V. Performance Evaluation

In this section, we present numerical data obtained as a result of applying equation.

$$MTTF = \sum_{i=1}^{Nq-1} i \left(\prod_{j=1}^{i} Rq\,(tQ,J) \right) (1 - Rq\,(tQ,i+1)) + Nq \prod_{j=1}^{Nq} Rq\,(tQ,j)$$

Our example HWSN consists of 3000 SN nodes and 100 CH nodes, deployed in a square area of A2 (200m×200m). Nodes are distributed in the area following a Poisson process with density λ_{SN} =30 nodes/(20 × 20 m2) and λ_{CH} =1node/(20×20 m2) at deployment time. The radio ranges r_{SN} and r_{CH} 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^{SN} 0 =0.8 Joules and E^{CH} 0 =10 Joules so that they exhaust energy at about the same time. The energy dissipation E_{elec} to run the transmitter and receiver circuitry is 50nJ/bit.

The energy used for transmit amplifier is to achieve an accept able signal to noise ratio (E_{amp}) is10pJ/bit/m2 for transmitted distances less than the threshold distance d_0 (75m) and 0.0013pJ/bit/m^4 for distances greater than d_0.The query arrival rate λ_q is a variable and is set to 1query/sec to reveal points of interest. The query deadline T_{req} is strict and set to between 0.3 and 1sec. The SN capture time is exponential distributed with rate λ_c such that $P_c = 1 - e^{-\lambda c \times T_{IDS}}$ .We test the effect of λ_c by varying the inter-arrival time in between attacks (T_{comp}) from 4 to 28 days, corresponding to an attack rate (λ_c) of once per 4 days to once per 28 days. The host IDS false positive probability and false negative probability (H_{pfp} and H_{pfn}) vary between 1% and 5% to reflect the host intrusion detection strength.

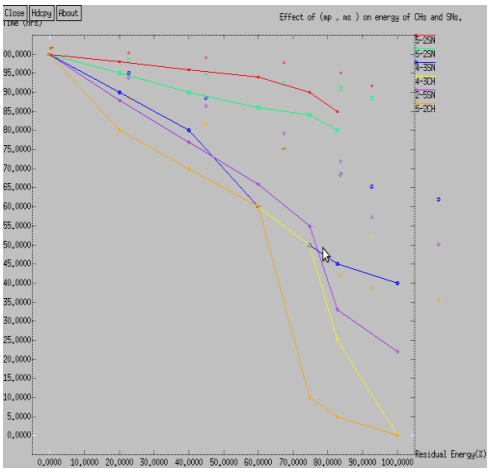


Fig: Effect of (m_p, m_s) on energy of CHs and SNs

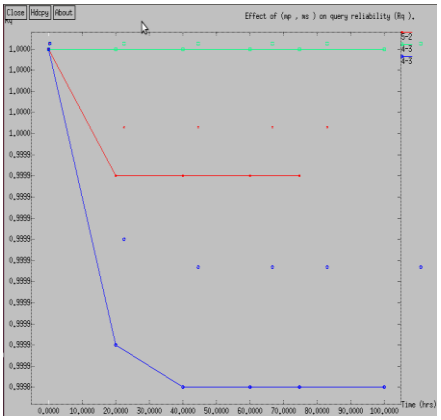


Fig: Effect of (m_p, m_s) on query reliability (Rq)

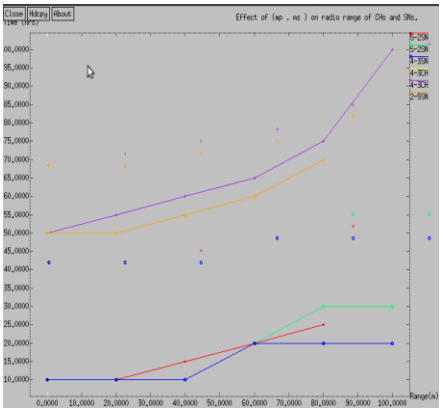


Fig: Effect of (m_p, m_s) on radio range of CHs and SNs

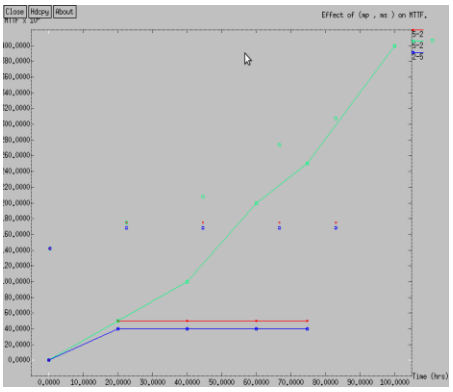


Fig: Effect of (m_p, m_s) on MTTF

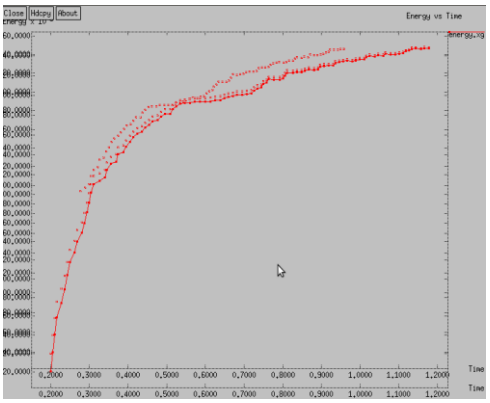


Fig: Effect of T_{IDS} on MTTF under low capture rate

VI. Conclusion

In this paper, we proposed a secure and reliable data aggregation protocol using trust relations among sensor nodes. The proposed protocol establishes a web of trust based on node misbehaviors. Data aggregators weight collected data using the web of trust to improve there liability of the aggregated data. Simulation results show that the proposed protocol ensures there liability of the aggregated data in the presence of compromised nodes. Moreover, the overhead imposed by the proposed protocol is shown to be tolerable.

References

[1] O.Younisand S.Fahmy, "HEED:a hybrid, energy-efficient, distributed clustering approach for adhoc 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," IEEETrans.MobileComput.,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 life time of query-based wireless sensor networks," IEEE Trans. Dependable Secure Computing,vol.8,no.2,pp.161–176,2011.

[4] M.Yarvis,N.Kushalnagar,H.Singh,A.Rangarajan,Y.Liu,andS.Singh,"Exploiting heterogeneity in sensor networks," in Proc.2005 IEEE Conf. Computer Commun.,vol.2,pp.878–890.

[5] H.M.AmmariandS.K.Das, "Promoting heterogeneity, mobility, and energy-aware Voronoi diagram in wireless sensor networks," IEEE Trans.ParallelDistrib.Syst.,vol.19,no.7,pp.995–1008,2008.

[6] X.DuandF.Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc.2005 IEEE Veh.Technol.Conf.,pp.2528–2532.

[7] S.Bo,L.Osborne,X.Yang,andS.Guizani, "Intrusion detection techniques in mobile adhoc and wireless sensor networks," IEEE Wireless Commun.Mag.,vol.14,no.5,pp.560–563,2007.

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

[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 adhoc networks," IEEE Trans.Reliab.,vol.59,no.1,pp.231–241,2010.

[10] A.P.R.daSilva,M.H.T.Martins,B.P.S.Rocha,A.A.F.Loureiro,L.B.Ruiz,andH.C.Wong,"Decentralized intrusion detection in wireless sensor networks," in Proc.2005ACMWorkshopQualityServiceSecurity Wireless Mobile Netw.

[11] Y.Zhou,Y.Fang,andY.Zhang, "Securing wireless sensor networks: a survey," IEEE Commun.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 Syst.,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 Commun.,vol.29,no.2,pp.216–230,2006.

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