Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks

Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, *Senior Member, IEEE* , and Tongtong Li

Abstract—This paper explores reliable data fusion in mobile access wireless sensor networks under Byzantine attacks. We consider the q-out-of-m rule, which is popular in distributed detection and can achieve a good tradeoff between the miss detection probability and the false alarm rate. However, a major limitation with it is that the optimal scheme parameters can only be obtained through exhaustive search, making it infeasible for large networks. In this paper, first, by exploiting the linear relationship between the scheme parameters and the network size, we propose simple but effective sub-optimal linear approaches. Second, for better flexibility and scalability, we derive a near-optimal closed-form solution based on the central limit theorem. Third, subjecting to a miss detection constraint, we prove that the false alarm rate of q-out-of-m diminishes exponentially as the network size increases, even if the percentage of malicious nodes remains fixed. Finally, we propose an effective malicious node detection scheme for adaptive data fusion under time-varying attacks; the proposed scheme is analyzed using the entropy-based trust model, and shown to be optimal from the information theory point of view. Simulation examples are provided to illustrate the performance of proposed approaches under both static and dynamic attacks.

Index Terms—Security in wireless sensor networks, Byzantine attacks, distributed detection

1 Introduction

Wireless sensor networks have received significant attention from the research community due to their impact on both military and civilian applications [1], [2], [3], [4]. Limited by the processing capability and power supply of the sensor nodes, incorporating security into wireless sensor networks has been a challenging task [5], [6], [7], [8], [9], [10]. A serious threat to wireless sensor networks is the Byzantine attack [11], [12], [13], [14], [15], [16], [17], where the adversary has full control over some of the authenticated nodes and can perform arbitrary behavior to disrupt the system. Discussions on related work can be found in *Section I of the supplementary file, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.74.*

In this paper, we consider reliable data fusion in wireless sensor networks with mobile access points (SENMA) [18] under both static and dynamic Byzantine attacks, in which the malicious nodes report false information with a fixed or time-varying probability, respectively. In SENMA, the mobile access point (MA) traverses the network and collects the sensing information from the individual sensor nodes. The major advantage of the SENMA architecture is that it ensures a line of sight path to the access point within the power range of the sensor nodes, allowing the information to be conveyed without routing. This feature makes it a resilient, scalable and energy efficient architecture for wireless sensor networks. In many cases, due to bandwidth and energy limitations, the sensors quantize their sensing result into a single bit [19], [20], [21], [22]. The MA receives the sensing reports and applies the fusion rule to make the final decision. One popular hard fusion rule used in distributed detection is the q-out-of-m scheme [20], [21], [23], in which the mobile access point randomly polls reports from m sensors, then decides that the target is present only if q or more out of the m polled sensors report '1'. It is simple to implement, and can achieve a good tradeoff between minimizing the miss detection probability and the false alarm rate. In-ideal scenarios, the optimal scheme parameters for the q-out-of-m fusion scheme are obtained through exhaustive search. However, due to its high computational complexity, the optimal q-out-of-m scheme is infeasible as the network size increases and/or the attack behavior changes. To overcome this limitation, effective sub-optimal schemes with low computational complexity are highly desired.

The main contributions of the paper can be summarized as follows: First, we propose a simplified, linear q-out-of-m scheme that can be easily applied to large size networks. The basic idea is to find the optimal scheme parameters at relatively small network sizes through exhaustive search, and then obtain the fusion parameters for large network size by exploiting the approximately linear relationship between the scheme parameters and the network size. It is observed that the proposed linear approach can achieve satisfying accuracy with low false alarm rate. However, there are chances of violating the problem constraint. To enforce the miss detection constraint and improve the data fusion accuracy, we further propose to use the linear approximation as the initial point for the optimal exhaustive search algorithm. With this

- *M. Abdelhakim, J. Ren, and T. Li are with the Department of Electrical and Computer Engineering, Michigan State University, 428 S. Shaw Lane, 2120 Engineering Building, East Lansing, MI 48824-1226. E-mail: {abdelhak, renjian, tongli}@egr.msu.edu.*
- *L.E. Lightfoot is with the Air Force Research Laboratory, Wright-Patterson Air Force Base, 2241 Avionics Circle WPAFB, Dayton, OH 45433. E-mail: Leonard.Lightfoot@wpafb.af.mil.*

Manuscript received 29 Oct. 2012; revised 4 Feb. 2013; accepted 21 Feb. 2013; date of publication 18 Mar. 2013; date of current version 21 Feb. 2014. Recommended for acceptance by R. Baldoni. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TPDS.2013.74

enhanced linear approach, near-optimal solutions can be obtained with much lower computational complexity compared with that of the pure exhaustive search approach.

Second, in an effort to search for an easier and more flexible distributed data fusion solutions that can easily adapt to unpredictable environmental changes and cognitive behavior of malicious nodes, we derive a closed-form solution for the q-out-of-m fusion scheme based on the central limit theorem. It is observed that the closed-form solution is a function of the network size, the percentage of malicious users, the malicious nodes' behavior, and the detection accuracy of the sensor nodes. We show that the closed-form solution delivers comparable results with that of the near-optimal solution obtained from the enhanced linear approach.

Third, we perform theoretical analysis for both the linear approach and the closed-form solution. We show that under a fixed percentage of malicious nodes, the false alarm rate for both approaches diminishes exponentially as the network size increases. This analysis reveals an interesting and important result: *even if the percentage of malicious nodes remains unchanged, larger size networks are much more reliable under malicious attacks.* It indicates that the network size plays a critical role in reliable data fusion. Moreover, we also find an upper bound on the percentage of malicious nodes that can be tolerated by the network under the q-out-of-m fusion rule. It turns out that this upper bound is determined by the sensors' detection probability and the attack strategies of the malicious nodes.

Finally, we propose a simple and effective malicious node detection approach, where the malicious sensors are identified by comparing the decisions of the individual sensors with that of the fusion center. It is observed that dynamic attacks generally take longer time and more complex procedures to be detected as compared to static attacks. It is also found that the proposed malicious detection procedure can identify malicious sensors accurately if sufficient observation time is allowed. The proposed approach is analyzed using an entropy-based trust model. We show that under the same system settings, the proposed malicious node detection approach is optimal from the information theory point of view. We further propose to adapt the fusion parameters based on the detected malicious sensors and their estimated probability of attack. It is shown that the proposed adaptive fusion scheme can improve the system performance significantly under both static and dynamic attack strategies.

2 Problem Formulation

2.1 Overall System Set-Up

We consider a centralized sensor network architecture, known as SENMA [24], where we assume that the network is composed of n power-limited sensor nodes and a powerful mobile access point. We assume that the nodes are randomly and uniformly distributed over the network, and the mobile access point traverses the network on a predefined trajectory to communicate with all the sensing nodes. The sensor network performs distributed detection. Each sensor node detects the presence of the target object by applying an application-dependent detection algorithm, such as energy detection [25], and sends its 1-bit hard decision report to the mobile access point ("1" means that the target is present), which makes the final decision accordingly. This hard decision model is adopted here for two reason: 1) To reduce the transmission and processing burden of the sensor network; 2) To enable more tractable analysis on the effect of the network size on the reliability of the distributed detection under Byzantine attacks.

If the network covers a large area, we divide the area into smaller sections, and apply the fusion rule over nodes that are within the same section. This setting ensures that, statistically, nodes within the same section have the same chance of detecting the target.

We assume that the network contains k malicious sensors. The percentage of malicious sensors, k/n, is denoted by α, which is assumed to be known or can be estimated at the mobile access point. When no prior knowledge of α exists, the MA would start with a majority vote[1] and obtain an estimate for α by comparing the individual sensing reports with the final decision.

We assume that each benign sensor node has a false alarm probability[2] P_f and a miss detection probability[3] P_m, while the malicious sensors have their own false alarm probability $\tilde{P}_f$ and miss detection probability $\tilde{P}_m$. These probabilities are determined by the environmental conditions and the sensors' capabilities to detect the target.

The MA uses the binary reports of the sensor nodes to make the final decision on whether the target is present or absent. This distributed detection problem can be modeled using the conventional binary hypothesis test, where the hypothesis H_0 represents the absence of the target, and the hypothesis H_1 represents the presence of the target. Here, we will first discuss different attack strategies that can be adopted by the malicious sensors, then present the problem formulation based on the q-out-of-m scheme.

2.2 Modeling of Possible Attack Strategies

There are different attack strategies that could be adopted by the malicious sensors. Let P_o be the probability that each malicious node intentionally reports the opposite information to its actual sensing decision. It is assumed that all malicious nodes have the same probability of attack in a particular sensing period. We classify the possible attack strategies into two categories:

1. *Static attack:* In this strategy, the malicious nodes send opposite data with an arbitrary probability P_o that is fixed, with $0 < P_o \leq 1$.
2. *Dynamic attack:* In this strategy, the malicious nodes change P_o after each attacking block, which is composed of one or more sensing periods. More specifically,

$$P_{o_n} = P_{o_{n-1}} + \Delta_1 x - \Delta_2(1-x), \tag{1}$$

where P_{o_n} is the value of P_o in the nth attacking block, x is a Bernoulli random variable that is equal to "1"

1. In majority vote, if more than half of the total sensor reported "1", then the final decision is "1".

2. The false alarm probability is the conditional probability that the target is said to be present, when it is not.

3. The miss detection probability is the conditional probability that the target is said to be absent, when it is present.

with probability P_x, Δ_1 and Δ_2 are the increment and decrement step size, respectively.

Taking the malicious nodes' own false alarm and miss detection probabilities into consideration, it turns out that the malicious sensors may have different probabilities of attack when the target is present and when the target is absent. We refer to them as the miss detection attack probability ($P_{a,m}$) and false alarm attack probability ($P_{a,f}$). More specifically, the overall miss detection attack probability is given by: $P_{a,m} = \overline{P_o}(1-\tilde{P}_m) + (1-\overline{P_o})\tilde{P}_m$, where $\overline{P_o} = P_o$ for static attacks, and equals to the average P_{o_n} over all attacking blocks for dynamic attacks. The false alarm attack probability is given by: $P_{a,f} = \overline{P_o}(1-\tilde{P}_f) + (1-\overline{P_o})\tilde{P}_f$. We define P_a as the overall attack probability of malicious sensors. If the state of nature is equal to "1" with probability p, then $P_a = pP_{a,m} + (1-p)P_{a,f}$. In the special case when the sensor nodes can perfectly detect the state of nature, i.e., $\tilde{P}_f = 0$ and $\tilde{P}_m = 0$, then $P_a = P_{a,m} = P_{a,f} = \overline{P_o}$.

2.3 Problem Formulation

For reliable data fusion in SENMA under Byzantine attacks, we propose to use the q-out-of-m fusion rule, in which the MA randomly polls m out of n reports, then decides that the target is present (H_1) only if q or more out of the m polled sensors report "1". The main reason is that other hard fusion rules, such as OR,[4] AND,[5] or the majority voting rule, might not achieve the compromise between minimizing the false alarm rate and the miss detection probability [20], especially under malicious attacks. Moreover, the q-out-of-m scheme parameters can be adapted based on the attacking behavior and percentage of malicious sensors. This inherent flexibility makes the q-out-of-m scheme superior to other hard fusion rules.

In this paper, we aim to obtain m and q to minimize the overall false alarm rate Q_f, while keeping the overall miss detection rate Q_m below a certain predefined value β. That is, our objective is to find the optimal m and q that can minimize Q_f, subject to the constraint $Q_m \leq \beta$. The problem can be formulated as follows:

$$\min_{m,q} Q_f(m,q)$$
$$s.t.\ Q_m(m,q) \leq \beta, \quad 1 \leq q \leq m \leq n, \quad q,m \in \mathbb{N}. \qquad (2).$$

It should be pointed out that there is always a tradeoff between minimizing the false alarm rate and the miss detection probability, therefore the parameter q should not be too small nor too large. Large q can improve the false alarm rate, but would increase the miss detection probability. Small q can achieve a higher detection probability, but would increase the false alarm rate.

Define $P_{k,n-k}^{d,m-d}$ as the probability of polling $m-d$ out of $n-k$ benign sensors and d out of k malicious sensors. That is, $P_{k,n-k}^{d,m-d} = \frac{\binom{k}{d}\binom{n-k}{m-d}}{\binom{n}{m}}$. According to our system model, the overall false alarm rate, Q_f, can be expressed as:

$$Q_f = \sum_{\substack{d=\max(0,\\ m+k-n)}}^{k} P_{k,n-k}^{d,m-d} \sum_{c=0}^{d} \binom{d}{c} P_{a,f}^{c}(1-P_{a,f})^{(d-c)} \times \sum_{j=\max(0,q-c)}^{m-d} \binom{m-d}{j} P_f^j (1-P_f)^{(m-d-j)}. \qquad (3)$$

If the m polled sensors contain d out of the k malicious nodes, then the false alarm occurs when c or more out of d malicious sensors attack and $q-c$ or more benign sensors send false alarms, where $0 \leq c \leq d$. It is noted that the minimum number of malicious reports being polled is $d = \max(0, m+k-n)$. That is, when the number of users polled, m, is greater than the number of benign users $(n-k)$, then there are at least $m-(n-k)$ malicious reports received by the MA. The overall probability of detection Q_d can be expressed as:

$$Q_d = \sum_{\substack{d=\max(0,\\ m+k-n)}}^{k} P_{k,n-k}^{d,m-d} \sum_{c=0}^{d} \binom{d}{c} (1-P_{a,m})^{c} P_{a,m}^{(d-c)} \times \sum_{j=\max(0,q-c)}^{m-d} \binom{m-d}{j} P_d^j (1-P_d)^{(m-d-j)}, \qquad (4)$$

where $P_d = 1 - P_m$ is the detection probability of the benign nodes, when the target is present. The overall miss detection probability Q_m is then obtained by $Q_m = 1 - Q_d$. Please refer to *Section II in the supplementary file, available online* for more discussions on the effect of the parameter q on Q_f and Q_m.

It is noted that finding the optimal m and q from (2) is a nonlinear integer optimization problem that is hard to be solved theoretically. The optimal approach is to perform exhaustive search over all possible m and q values, and then choose the (m_o, q_o) pair that results in the lowest false alarm rate while satisfying the miss detection constraint. The computational complexity of the optimal exhaustive search is $O(n^2)$ [26], which would be infeasible for real-time data fusion in large networks. Therefore, we aim at finding simpler but accurate methods to obtain the scheme parameters that solve (2).

3 Simplified Data Fusion Scheme—The Linear Approach

In this section, we will first highlight some observations based on the optimal q-out-of-m scheme, and then present the simplified algorithms that can be easily applied to large-scale networks.

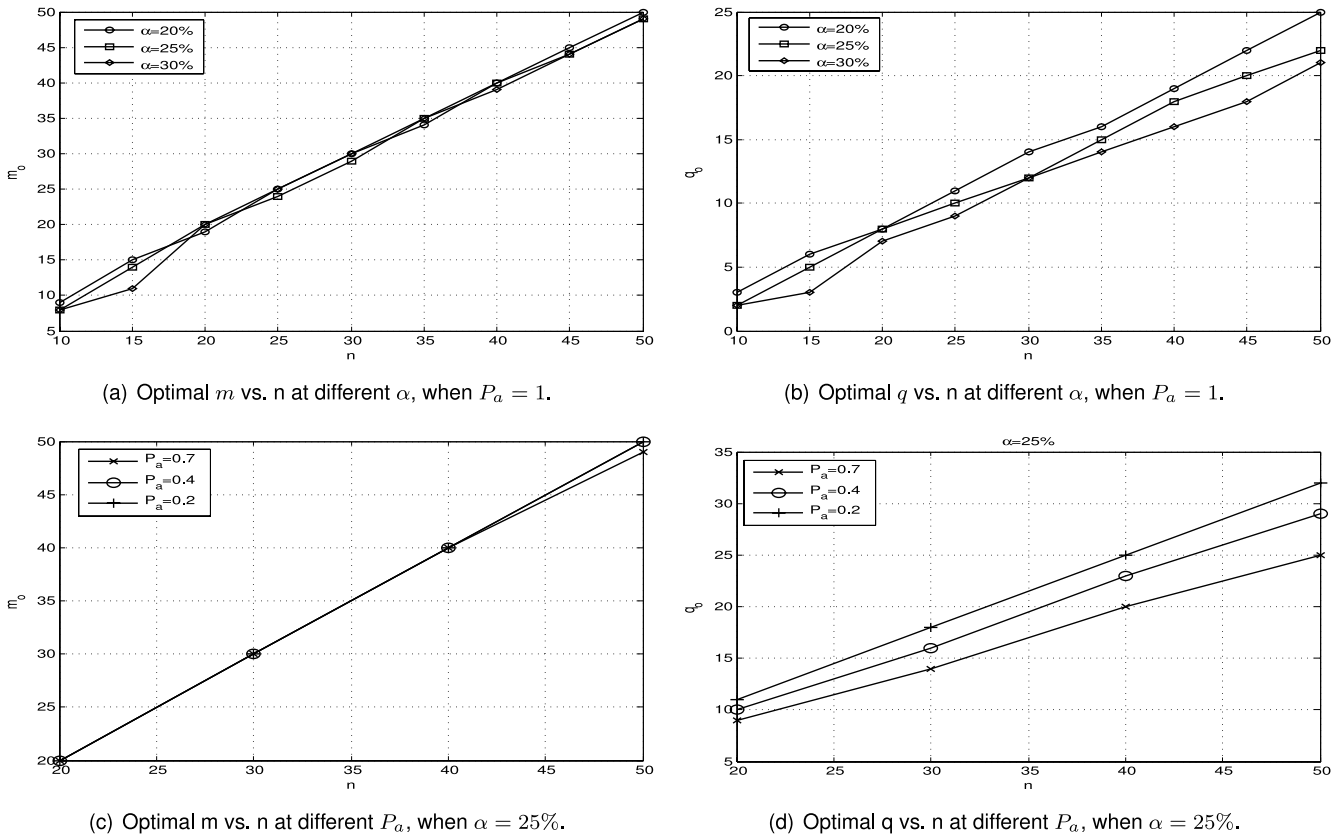
3.1 Observations

To develop effective sub-optimal schemes with low computational complexity, it is important to know how the parameters m and q change with the system variables, such as α and n. In this section, we consider the case where the malicious sensors attack with probability P_a. We calculate the optimal parameters at different P_a values, under different network sizes and different percentages of malicious sensors. The following observations are made [27]:

Observation 1. The optimal m is almost independent of the percentage of malicious nodes, and has a linear

4. OR rule: if at least one sensor reports "1", then the decision is "1"; otherwise, the decision is "0".

5. AND rule: if all sensors report "1", then the decision is "1"; otherwise, the decision is "0".



(a) Optimal m vs. n at different α, when $P_a = 1$.

(b) Optimal q vs. n at different α, when $P_a = 1$.

(c) Optimal m vs. n at different P_a, when $\alpha = 25\%$.

(d) Optimal q vs. n at different P_a, when $\alpha = 25\%$.

Fig. 1. Optimal scheme parameters (m_o, q_o) versus the network size at different percentage of malicious nodes (α) and different probability of attack (P_a), when $\beta = 0.01$, $P_f = 0.1$, $P_d = 0.775$, $P_{a,m} = P_{a,f}$.

relationship with n. In fact, it is always equal to or very close to n, as shown in Figs. 1a and 1c, which implies that the reports of almost all the sensors should be considered in the optimal q-out-of-m fusion scheme.[6]

This observation enables us to reduce the problem to finding the best q when $m = n$, which lowers the computational complexity from $O(n^2)$ to $O(n)$.

Observation 2. The optimal value of q follows an approximately linear function of n with different slopes depending on the percentage of the malicious nodes and the probability of attack, as shown in Figs. 1b and 1d.

Motivated by these observations, we develop simplified approaches to obtain the q-out-of-m fusion parameters with low complexity that can be easily applied to large network sizes.

3.2 The Linear Approach

In this section, we propose a simplified q-out-of-m scheme by exploiting the linear relationship between the scheme parameters and the network size. The main idea is that we can get the optimal scheme parameters at relatively small network sizes, and use them as reference points. These optimal (m, q) pairs for the different network sizes, P_a values, and α ratios, can be obtained and stored in a look-up table, then used to get the suboptimal scheme parameters for large network sizes. We propose to set $m = n$ and use the following linear function of n to obtain q [27]:

$$\hat{q}_{n,\alpha} = \lceil q_{n_0,\alpha} + S_o(\alpha)(n - n_0) \rceil, \tag{5}$$

where $S_o(\alpha)$ is the slope of the optimal q_o versus n curve at a particular attack probability given that the percentage of the malicious nodes is α, $\hat{q}_{n,\alpha}$ is the suboptimal q value at a network size n, and $q_{n_o,\alpha}$ is the optimal q value at a relatively small network size n_0 and it serves as a reference point. Both $\hat{q}_{n,\alpha}$ and $q_{n_o,\alpha}$ are at α percent of malicious sensors. $\lceil x \rceil$ is the smallest integer larger than or equal to x. Note that the optimal q depends on the false alarm and miss detection probabilities of the sensor nodes, hence a periodic update of the reference points and related slopes would be required in time-varying environments.

While the linear approach can deliver very good performance, there are chances of violating the problem constraint. Therefore, we propose an enhanced linear approach to guarantee that the choice of q satisfies the miss detection probability constraint. Please see *Section III in the supplementary file, available online*.

The absence of a well-defined closed-form solution makes it difficult to adapt q based on the environmental conditions and the malicious behavior. To find q for different network settings, the slopes and the reference points should always be updated using exhaustive search. This

6. However, this is no longer the case when malicious node detection scheme is employed, as the reports of the malicious sensors would be discarded. Malicious detection will be considered in Section 6.

could be tedious when the environment is fast-varying. To solve this problem, in the following section, we derive a closed-form expression for q.

4 A Closed-Form Solution

In this section, we derive a closed-form solution of q for the q-out-of-m fusion rule under both static and dynamic attacks. We exploit the observations of the optimal exhaustive search by setting $m = n$, as illustrated in the previous section.

Recall that the malicious sensors have miss detection and false alarm attack probabilities, $P_{a,m}$ and $P_{a,f}$, respectively. For notation simplicity, we assume that these two probabilities are equal, that is, $P_{a,m} = P_{a,f} = P_a$. It is worth mentioning that the analysis can be easily extended to the case where $P_{a,m} \neq P_{a,f}$. We assume that all sensing reports are independent. It is noted that the distribution of each sensing report is determined by the environment and the behavior of the corresponding sensor node. Let the sensing report of node i be $u_i \epsilon \{0, 1\}$, where $i = \{1, \ldots, n\}$. If node i is benign, then u_i is a Bernoulli random variable characterized by detection probability P_d if the target is present, or the false alarm rate P_f if the target is absent; if node i is malicious, then u_i is a Bernoulli random variable characterized by the parameter $1 - P_a$ if the target is present, or P_a if the target is absent.

The aggregated result at the MA is given by, $U = \sum_{i=1}^{n} u_i$ The random variable U represents the number of 1's that the access point received. To apply the q-out-of-m fusion rule, U is compared to q. If $U \geq q$, the final decision is that the target is present (i.e., decide H_1); otherwise, the final decision is that the target is absent (i.e., decide H_0).

Our closed-form solution is based on the central limit theorem, where the aggregated result at the access point is approximated as a Gaussian random variable. In fact, we have the following result.

Proposition 1. *Suppose a network of size n containing both benign sensors and malicious sensors, where the percentage of malicious sensors is α. The benign sensors have a detection probability P_d, and the malicious sensors attack with a probability P_a. Assuming the q-out-of-m fusion rule is applied subject to a predefined miss detection constraint β, then the lowest false alarm rate can be achieved when $q = \lfloor an + \sqrt{bn} Q^{-1}(1-\beta) \rfloor$. Here, $a = (1-\alpha)P_d + \alpha(1-P_a)$, $b = (1-\alpha)P_d(1-P_d) + \alpha(1-P_a)P_a$, and $Q^{-1}(.)$ is the inverse Q function.*[7]

The proof of Proposition 1 is provided in *Section IV of the supplementary file, available online*. Discussions on the different q obtained by the proposed approaches can also be found in the *Section V of the supplementary file, available online*.

Next, we consider the maximum percentage of malicious nodes that can be tolerated by the network using the q-out-of-m fusion rule. More specifically, we have the following result: *For reliable data fusion using the q-out-of-m rule, the percentage of malicious users has to satisfy $\alpha < \frac{P_d}{P_d + P_a}$, where P_d is the probability of detection of the sensors and P_a is the attack probability of the malicious nodes.* The upper bound on α that can be tolerated by the network is derived in *Section VI of the supplementary file, available online*.

7. The Q function is defined as: $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{x^2}{2}} dx$.

5 Analytical Bounds for the Proposed Approaches

In this section, we derive the analytical bound for the q-out-of-m scheme based on the closed-form solution and the linear approach, and *show that the accuracy of the q-out-of-m scheme increases exponentially as the network size increases, even if the percentage of malicious users remains the same.* We consider the linear approach first, for which we have:

Proposition 2. *Using the linear q-out-of-m approach, the overall false alarm rate diminishes exponentially as the network size n goes to infinity. More specifically, when n is very large and $P_f < \frac{q-k}{n-k}$, then $Q_f \leq \exp\{-(An + B)\}$, where A and B are constants, and $A > 0$.*

The proof of Proposition 2 is provided in *Section VII of the supplementary file, available online*.

For the closed-form solution, we have:

Proposition 3. *For a fixed percentage of malicious users and under the same attack strategy, the overall false alarm rate using the closed-form q-out-of-m approach diminishes exponentially as the network size n goes to infinity. More Specifically, for large n and $P_f < \frac{q-k}{n-k}$, $\tilde{Q}_f \leq \exp[-\frac{1}{2}\frac{(a-c)^2}{d} n]$, where a, c and d are constants.*

The proof of Proposition 3 is provided in *Section VIII of the supplementary file, available online*.

Discussions. (i) Our analytical results provided in this section indicate that: when the q-out-of-m rule is used for data fusion, then the false alarm rate diminishes exponentially as the network size increases even if the percentage of malicious sensors remains the same. This implies that for a fixed α, we can improve the network performance significantly by increasing the network size.

(ii) *Explanation on the condition in Propositions 2-3:* The condition "$P_f < \frac{q-k}{n-k}$" is equivalent to "$q - k > P_f(n-k)$". The physical meaning of this condition can be explained in two ways: First, in order to achieve arbitrarily low overall false alarm probability by the q-out-of-m fusion rule, the individual false alarm rates of the benign nodes should be less than a certain limit. This limit is equal to the ratio between the least number of benign nodes in the set of q nodes relied on in the q-out-of-m scheme $(q-k)$, to the total number of benign nodes $(n-k)$. Second, since each benign node has a none zero false alarm rate P_f, to reduce the overall false alarm rate, sufficient number of benign nodes need to be taken into account so the "averaged" result will lead to a low overall false alarm rate.

6 Malicious Node Detection and Adaptive Fusion

In this section we propose to enhance the system performance through malicious node detection, where the hostile behavior is identified and the malicious sensors are discarded from the final decision making. Furthermore, we propose an adaptive fusion procedure, where the fusion

parameters are tuned based on the attack behavior and the percentage of the malicious sensors.

6.1 The Malicious Node Detection Scheme

Let I_{mal} be the set of the malicious nodes, and O_{N_s} denotes the reports of all nodes till the sensing period N_s. When the attack strategy is known, and the percentage of malicious nodes is fixed, a traditional approach to find the malicious set, I_{mal}, is to maximize the *a posterior* probability of I_{mal} given the observations O_{N_s} [28]. That is, the detected malicious set $\hat{I}_{mal} = \arg\max_{I_{mal}} P(I_{mal}|O_{N_s})$, where $P(I_{mal}|O_{N_s})$ is the conditional probability that the malicious set is I_{mal} given all the reports O_{N_s}. However, this detection approach is difficult to be implemented since it requires searching over all possible sets of I_{mal}.

In this section, we propose a simple malicious node detection scheme, where the sensors' decision reports are used to identify the malicious nodes and estimate their attack behavior. Let $P_{a,f}(i)$ and $P_{a,m}(i)$ denote the probabilities that the ith node attacks when the target is absent and present, respectively. Let $\hat{P}_{a,f}(i)$ and $\hat{P}_{a,m}(i)$ be their estimated versions. We estimate $P_{a,f}(i)$ and $P_{a,m}(i)$ by using two counters for each node at the mobile access point. More specifically, for node i,

- $T_{i,o}$: represents the number of times node i sends "0" when the final decision is "1".
- $T_{i,1}$: represents the number of times node i sends "1" when the final decision is "0".

These counters are updated after each sensing period by comparing the final decision (obtained using the q-out-of-m rule) with the individual sensing reports.

Assuming the observation interval is N sensing periods, and the number of observations where the access point decides that the target is present and absent are N_1 and N_0, respectively. Then, if the node is benign, $\frac{T_{i,o}}{N_1}$ and $\frac{T_{i,1}}{N_0}$ would be indications for the ith node's miss detection probability and false alarm rate, respectively. On the other hand, if node i is malicious, $\frac{T_{i,o}}{N_1}$ and $\frac{T_{i,1}}{N_0}$ will be estimates for $P_{a,m}(i)$ and $P_{a,f}(i)$, respectively. Please refer to *Section XI in the supplementary file, available online* for more specific discussions.

We define the thresholds $\lambda_{p,f}$ and $\lambda_{p,m}$ as:

$$\lambda_{p,f} = P_f + \delta_{f,0}, \qquad \lambda_{p,m} = P_m + \delta_{m,0}, \tag{6}$$

where P_f and P_m are the benign nodes' false alarm and miss detection probabilities, $\delta_{f,0}$ and $\delta_{m,0}$ represent the tolerance in the estimated false alarm rate and miss detection probability of the nodes.

The malicious node detection procedure has two levels:

- *Level 1: Discard the suspicious reports*. If $\frac{T_{i,o}}{N_1} \geq \lambda_{p,m}$ or $\frac{T_{i,1}}{N_0} \geq \lambda_{p,f}$, the node's report is discarded from the current decision process, but its counters will continue to be updated in the next sensing periods.
- *Level 2: Discard the unreliable nodes*. If $\frac{T_{i,o}}{N_1} \geq P_m + \delta_1$ or $\frac{T_{i,1}}{N_0} \geq P_f + \delta_2$, where δ_1 and δ_2 are relatively large, then the corresponding node will be discarded from the sensing process. The nodes' counters will continue to be updated to estimate the attack probability.

It should be noted that N needs to be greater than or equal to a certain threshold N_{th} before taking the decision to discard any node. N_{th} should be chosen to ensure the accuracy of the time averages, $\hat{P}_{a,f}(i)$ and $\hat{P}_{a,m}(i)$. When $P_{a,f}(i)$ and $P_{a,m}(i)$ are in the orders of 10^{-1}, it is safe to choose $N_{th} \geq 100$. As will be illustrated in Section 7, the detection of the malicious nodes launching dynamic attacks is generally more difficult and takes longer time than the detection of the malicious nodes performing static attacks.

6.2 The Adaptive Fusion Algorithm

Adaptive fusion can be achieved by updating the value of the q-out-of-m fusion parameters based on the average probability of attack. Recall that $\hat{I}_{mal}$ is the set of detected malicious nodes, then $|\hat{I}_{mal}|$ is the total number of sensors detected to be malicious. The estimated average attack probability is given by

$$\hat{P}_a = \frac{1}{|\hat{I}_{mal}|} \sum_{i=1}^{|\hat{I}_{mal}|} \hat{P}_a(\hat{I}_{mal}(i)), \tag{7}$$

where $\hat{I}_{mal}(i)$ is the ith detected malicious sensor and $\hat{P}_a(\hat{I}_{mal}(i)) = \frac{T_{\hat{I}_{mal}(i),o} + T_{\hat{I}_{mal}(i),1}}{N}$. Then, q is tuned using Proposition 1 with the new problem settings, where $n - |\hat{I}_{mal}| \Rightarrow n$, $k - |\hat{I}_{mal}| \Rightarrow k$, $\alpha = k/n$ and $P_a = \hat{P}_a$.

We define η_d and η_f as the detection accuracy and false alarm rate of the malicious node detection scheme, respectively. That is,

$$\eta_d \triangleq \frac{N_{MM}}{k}, \quad \eta_f \triangleq \frac{N_{BM}}{n-k}, \tag{8}$$

where N_{MM} is the number of malicious nodes detected to be malicious, N_{BM} is the number of benign nodes mistakenly regarded as malicious, k is the total number of malicious sensors and $(n-k)$ is the number of benign sensors. Note that $|\hat{I}_{mal}| = N_{MM} + N_{BM}$. It will be shown in Section 7 that with sufficient observation time, the proposed detection scheme can achieve high η_d and low η_f under static and dynamic attacks.

6.3 Analysis from the Entropy Point of View

In the proposed malicious node detection approach, each node's behavior is determined based on the uncertainty in the accuracy of its sensing report. Since uncertainty is generally measured by entropy, in this section, we analyze the proposed approach using the entropy-based trust model [29].

First, for each node $i \in \{1, 2, \ldots, n\}$, we define two trust metrics $Trust_f(i)$ and $Trust_m(i)$ to represent the uncertainty in the node's accuracy when the target is absent and present, respectively,

$$Trust_f(i) \triangleq \begin{cases} 1 - H(\hat{P}_{a,f}(i)), & \text{if } \hat{P}_{a,f}(i) < 0.5, \\ H(\hat{P}_{a,f}(i)) - 1, & \text{if } \hat{P}_{a,f}(i) \geq 0.5, \end{cases} \tag{9}$$

where $H(\hat{P}_{a,f}(i))$ is the entropy which represents the uncertainty that node i intentionally reports a false "1" when the actual state of nature is "0". That is,

TABLE 1
Equivalence between the Entropy Based Trust Model and the Proposed Malicious Node Detection

Cases	Entropy-based trust model vs. the proposed malicious node detection approach
1. Discard suspicious reports	$Trust_f(i) \le \lambda_{e,f} \Leftrightarrow \hat{P}_{a,f}(i) \ge \lambda_{p,f}$
	$Trust_m(i) \le \lambda_{e,m} \Leftrightarrow \hat{P}_{a,m}(i) \ge \lambda_{p,m}$
2. Discard unreliable nodes	$Trust_f(i) \le 0 \Leftrightarrow \hat{P}_{a,f}(i) \ge 0.5$
	$Trust_m(i) \le 0 \Leftrightarrow \hat{P}_{a,m}(i) \ge 0.5$

$$H\big(\hat{P}_{a,f}(i)\big) = -\hat{P}_{a,f}(i)\log_2\big[\hat{P}_{a,f}(i)\big] - \big[1-\hat{P}_{a,f}(i)\big]\log_2\big[1-\hat{P}_{a,f}(i)\big]. \quad (10)$$

$Trust_m(i)$ is defined in a similar way by replacing $\hat{P}_{a,f}(i)$ in equation (9) with $\hat{P}_{a,m}(i)$.

The entropy trust metrics are in the range $[-1, 1]$, where negative values mean that the attack probability of the corresponding node is greater than 0.5. The trust metrics are equal to "1" when the corresponding node is benign with a perfect detection accuracy.

Note that P_f and P_m are generally small quantities, and we can assume $P_f + \delta_{0,f} < 1/2$ and $P_m + \delta_{0,m} < 1/2$. Define $\lambda_{e,f}$ and $\lambda_{e,m}$ as:

$$\lambda_{e,f} \triangleq 1 - H(P_f + \delta_{0,f}), \quad \lambda_{e,m} \triangleq 1 - H(P_m + \delta_{0,m}). \quad (11)$$

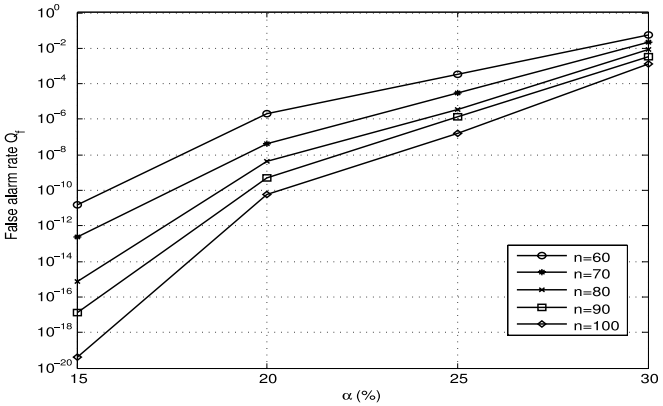
Compare (11) and (6), we can see that the proposed malicious node detection approach can be mapped to the entropy-based trust model. The equivalence is further illustrated in Table 1.

Our discussions above show that under the same settings for $\delta_{0,f}$, $\delta_{0,m}$, δ_1 and δ_2, the proposed malicious node detection scheme is equivalent to the detection approach based on the entropy-based trust model. This implies that the proposed malicious node detection scheme is optimal from the information theory point of view.

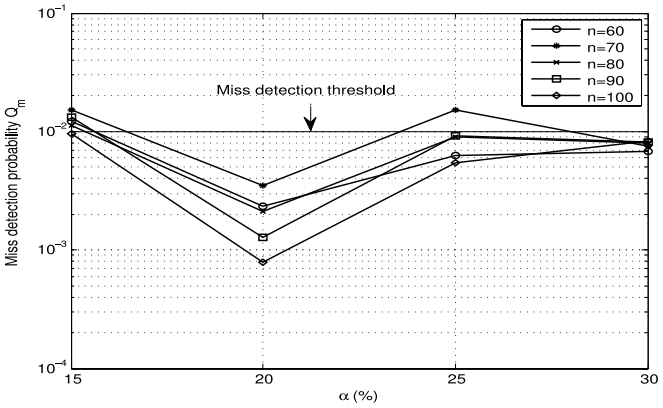
7 Simulation Results

In this section, we illustrate the performance of the proposed approaches through simulation examples. In the simulations, we assume that the miss detection limit is $\beta = 0.01$, the hypothesis H_1 happens with probability $p = 0.5$. The false alarm rate and the miss detection probability of each benign sensor are assumed to be $P_f = 0.1$ and $P_d = 0.775$. These false alarm and miss detection values are obtained assuming that the sensors employ energy detection, when the SNR level is 5 dB and the time-bandwidth product is 5 [30]. For the static attack strategy, we set $P_o = 1$. For the dynamic attack strategy, we set $\Delta_1 = \Delta_2 = 0.2$, $P_{o_1} = 0.7$, $P_x = 0.5$, and the number of sensing periods per attacking block is $T = 10$.

Example 1. *Linear approaches and comparison with existing methods*. In this example, the performance of the linear and the enhanced linear approaches are evaluated, and we also compare them with existing AND rule, OR rule, and majority voting fusion approaches. We assume that the malicious nodes can detect the target perfectly and always report false information (i.e., $P_{a,m} = 1$, $P_{a,f} = 1$). At different values of α, $S_o(\alpha)$ is calculated from Fig. 1. The reference points are at $n_o = 35$. The false alarm rate and the corresponding miss detection probability of the linear approach for different values of n and α are shown in Figs. 2a and 2b, respectively. It is clear that in most cases, the miss detection constraint is met. Slight increase in the miss detection over β happens at $\alpha = 15\%$ and 25%. One solution to this problem is to use the enhanced linear approach discussed in *Section III of the supplementary file, available online*.



(a) The false alarm rate.

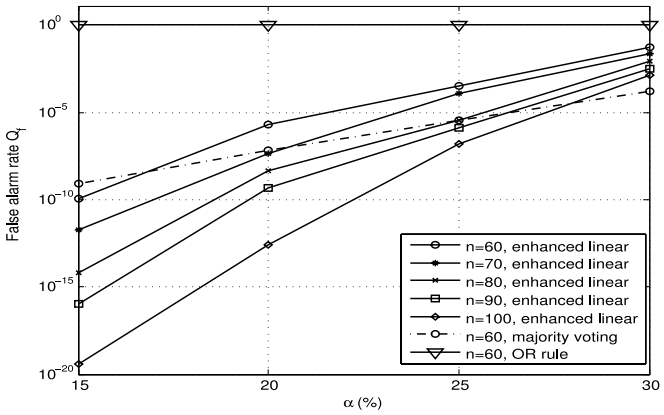


(b) The miss detection probability.

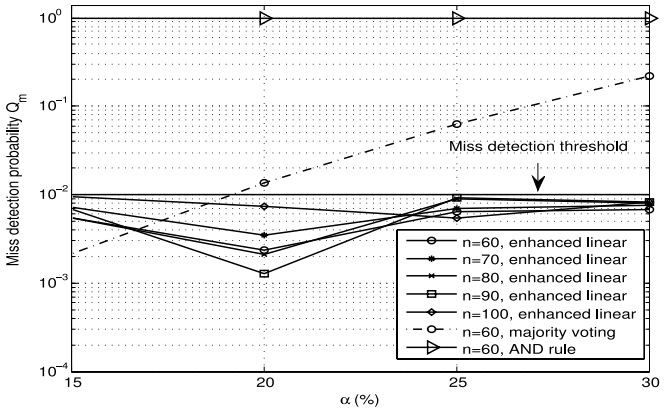
Fig. 2. The false alarm rate and miss detection probability using the linear approach.

Figs. 3a and 3b show the false alarm rate and the miss detection probability, respectively, at different percentages of malicious nodes, when the iterative enhanced linear approach is used to find the fusion parameter. Comparing Fig. 3b with Fig. 2b, it can be seen that the miss detection constraint is enforced when the enhanced procedure is applied. It can also be shown from both Figs. 2a and 3a that the false alarm rate improves as the network size increases even under the same percentage of malicious nodes.

In comparison with existing approaches, it is shown in Fig. 3b that the majority voting rule cannot guarantee the miss detection requirement. Moreover, AND rule results in a very high miss detection probability, although it can achieve low false alarm rate. On the other hand, OR rule results in a very high false alarm rate, although it can

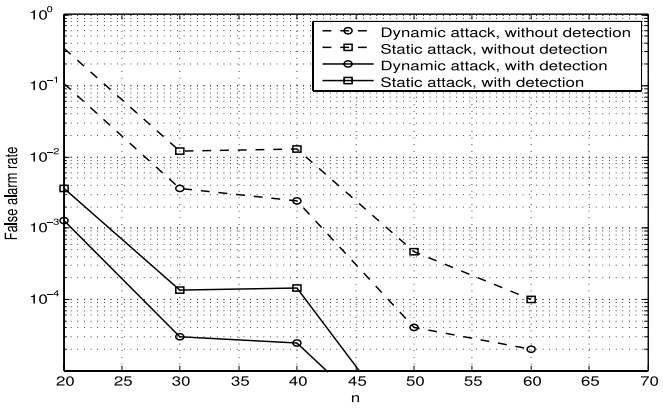


(a) The false alarm rate.

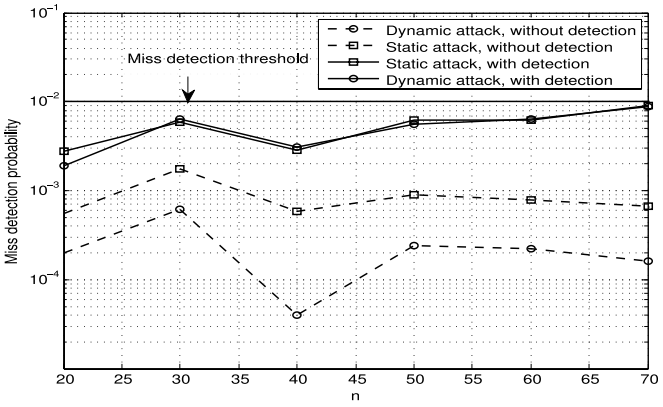


(b) The miss detection probability.

Fig. 3. The false alarm rate and the miss detection probability using the enhanced linear approach, and comparisons with AND rule, OR rule and majority voting rule. In general, AND rule results in very high miss detection probability, although it can achieve low false alarm rate. On the other hand, OR rule results in a very high false alarm rate, although it can achieve low miss detection probability.



(a) The false alarm rate.



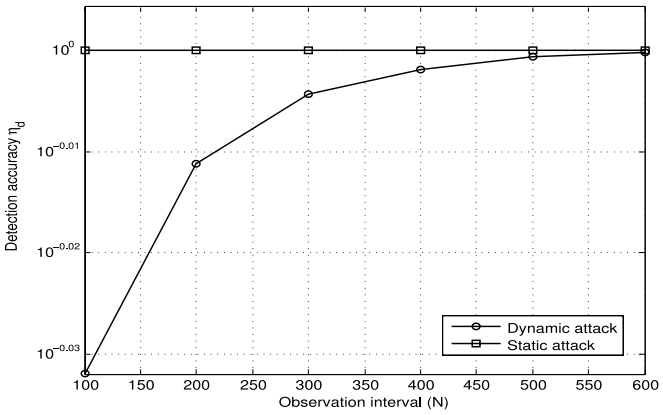
(b) The miss detection probability.

Fig. 4. The false alarm rate and miss detection probability under static and dynamic attacks with and without the malicious node detection scheme.

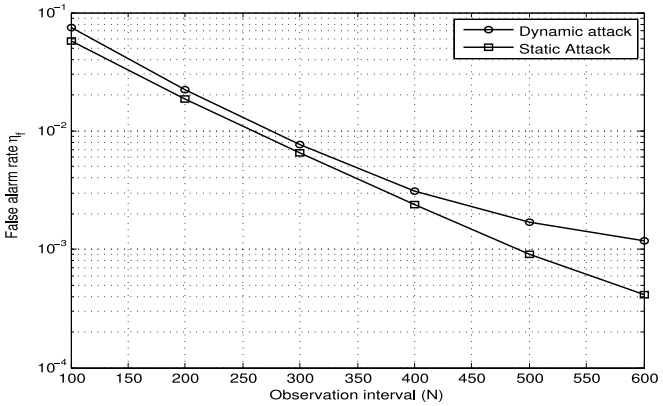
achieve low miss detection probability. Hence, they are not reliable under malicious attacks.

Example 2. *The closed-form solution without malicious node detection*. In this example, we assume that $\alpha = 25\%$, and the malicious nodes have $\tilde{P}_f = P_f$ and $\tilde{P}_m = 1 - P_d$. The access point assumes that the attack probability is "1", and obtain q accordingly. We assume that the percentage of malicious sensors is known or can be estimated at the access point. It is shown in Fig. 4a that when the malicious detection approach is not employed, the performance is worst under the static attack strategy with $P_o = 1$. It is observed that the false alarm rate is lower for the considered dynamic attacks as compared to the static attack. This is because that when the probability of attack is time varying, it could be very low in some sensing periods. It can be observed from Fig. 4a that at a fixed percentage of malicious nodes, the false alarm rate decreases rapidly as the network size increases. This echoes our analytical results presented in Section 5. The miss detection probability versus the network size is plotted in Fig. 4b. It is clear that the miss detection constraint is met, and there is a good margin for improvement that can be achieved using the adaptive fusion scheme. This margin is mainly due to the choice of q, where the access point assumed that the attack probability is "1".

Example 3. *Adaptive fusion: closed-form solution with malicious node detection*. In this example, we use the same settings as in Example 2. Malicious node detection is applied and the value of q is adapted based on the detected malicious behavior. Here, we set $\delta_{0,f} = 0.07$, $\delta_{0,m} = 0.2$, $\delta_1 = 0.4$, and $\delta_2 = 0.3$. Fig. 4a shows the overall false alarm rate averaged over 10^4 observation periods when $N_{th} = 100$. The results are further averaged over 10^2 iterations to get more accurate results. It can be seen that significant performance improvement is achieved for both static and dynamic attacks when the adaptive fusion with malicious node detection is employed. Fig. 4b shows that the miss detection constraint is satisfied for all cases. The non-smoothness of the curves is mainly due to the tuning of the integer-valued scheme parameters to satisfy the miss detection constraint. It should be noted that the thresholds $\delta_{0,f}$, $\delta_{0,m}$ have a direct impact of the performance of the malicious node detection scheme and they could be further optimized to improve the performance.



(a) The detection accuracy



(b) The false alarm rate.

Fig. 5. The effect of the observation interval (N) on the detection accuracy η_d and the false alarm rate η_f for static and dynamic attacks using $N_{th} = 100$, $n = 30$. The results are averaged over 4×10^3 iterations.

In Fig. 5a, we show the effect of the observation interval N on the detection accuracy of the malicious node detection scheme (η_d). It can be seen that malicious nodes launching dynamic attack require longer observation interval to be detected than nodes adopting static attack. Fig. 5a demonstrates that the proposed malicious node detection scheme is efficient and highly accurate. In Fig. 5b, the false alarm rate of the malicious node detection scheme (η_f) is plotted versus the observation interval. As expected, it is shown that η_F decreases as more observations are available at the access point. The effect of the observation threshold N_{th} on η_f is illustrated in *Section X of the supplementary file, available online*.

8 Conclusions

In this paper, we considered the q-out-of-m fusion rule for SENMA networks under Byzantine attacks. Both static and dynamic attack strategies were discussed. We proposed simplified q-out-of-m fusion schemes by exploiting the linear relationship between the scheme parameters and the network size. We also derived a near-optimal closed-form solution for the fusion threshold based on the central limit theorem. An important observation is that, even if the percentage of malicious sensors remains fixed, the false alarm rate diminishes exponentially with the network size. This implies that for a fixed percentage of malicious nodes, we can improve the network performance significantly by increasing the density of the nodes. Furthermore, we obtained an upper bound on the percentage of malicious nodes that can be tolerated using the q-out-of-m rule. It is found that the upper bound is determined by the sensors' detection probability and the attack strategies of the malicious nodes. Finally, we proposed an effective malicious node detection scheme for adaptive data fusion under time-varying attacks. The detection procedure is analyzed using the entropy-defined trust model, and has shown to be optimal from the information theory point of view. It is observed that nodes launching dynamic attacks take longer time and more complex procedures to be detected as compared to those conducting static attacks. The adaptive fusion procedure has shown to provide significant improvement in the system performance under both static and dynamic attacks. Further research can be conducted on adaptive detection under Byzantine attacks with soft decision reports.

References

[1] Y.-C. Wang and Y.-C. Tseng, "Distributed Deployment Schemes for Mobile Wireless Sensor Networks to Ensure Multilevel Coverage," *IEEE Trans. Parallel and Distributed Systems*, vol. 19, no. 9, pp. 1280-1294, Sept. 2008.

[2] P. Barooah, H. Chenji, R. Stoleru, and T. Kalmar-Nagy, "Cut Detection in Wireless Sensor Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 3, pp. 483-490, Mar. 2012.

[3] A. Bharathidasas and V. Anand, "Sensor Networks: An Overview," technical report, Dept. of Computer Science, Univ. of California at Davis, 2002.

[4] C. Chong and S. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proc. IEEE*, vol. 91, no. 8, pp. 1247-2056, Aug. 2003.

[5] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "Spins: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, pp. 521-534, http://dx.doi.org/10.1023/A:1016598314198, Sept. 2002.

[6] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks," *Proc. Second Int'l Conf. Embedded Networked Sensor Systems*, pp. 162-175, http://doi.acm.org/10.1145/1031495.1031515, 2004.

[7] L. Lightfoot, J. Ren, and T. Li, "An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Electro/Information Technology*, pp. 233-238, May 2007.

[8] I. Rodhe, C. Rohner, and A. Achtzehn, "n-lqa: n-Layers Query Authentication in Sensor Networks," *Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems*, pp. 1-6, Oct. 2007.

[9] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," *Proc. IEEE 27th Conf. Computer Comm.*, pp. 1418-1426, Apr. 2008.

[10] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," *Proc. 13th Int'l Conf. Network-Based Information Systems (NBiS '10)*, pp. 313-320, Sept. 2010.

[11] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical in-Network Aggregation in Sensor Networks," *Proc. 13th ACM Conf. Computer and Comm. Security (ACM CCS '06)*, pp. 278-287, 2006.

[12] H. Kumar, D. Sarma, and A. Kar, "Security Threats in Wireless Sensor Networks," *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 6, pp. 39-45, June 2008.

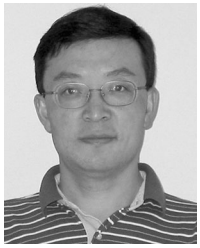
[13] B. Awerbuch, R. Curtmola, H.D., N.-R.C., and R.H., "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks," Technical Report Version 1, Dept. of Computer Science, Johns Hopkins Univ., Mar. 2004.

[14] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attack in Large Wireless Sensor Networks," *Proc. IEEE Military Comm. Conf.*, pp. 1-4, Oct. 2006.

[15] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attacks," *IEEE Trans. Signal Processing*, vol. 57, no. 1, pp. 16-29, Jan. 2009.
[16] O. Kosut and L. Tong, "Distributed Source Coding in the Presence of Byzantine Sensors," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2550-2565, June 2008.
[17] G. Latif-Shabgahi, "A Novel Algorithm for Weighted Average Voting Used in Fault Tolerant Computing Systems," *Microprocessors and Microsystems*, vol. 28, no. 7, pp. 357-361, 2004.
[18] G. Mergen, Z. Qing, and L. Tong, "Sensor Networks with Mobile Access: Energy and Capacity Considerations," *IEEE Trans. Comm.*, vol. 54, no. 11, pp. 2033-2044, Nov. 2006.
[19] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," *IEEE Trans. Signal Processing*, vol. 59, no. 2, pp. 774-786, Feb. 2011.
[20] R. Viswanathan and V. Aalo, "On Counting Rules in Distributed Detection," *IEEE Trans. Acoustics, Speech and Signal Processing*, vol. 37, no. 5, pp. 772-775, May 1989.
[21] R. Niu and P. Varshney, "Performance Analysis of Distributed Detection in a Random Sensor Field," *IEEE Trans. Signal Processing*, vol. 56, no. 1, pp. 339-349, Jan. 2008.
[22] V. Aalo and G. Efthymoglou, "Decision Fusion Schemes for Wireless Sensor Networks Operating in a Nakagami-m Fading Environment," *Proc. IEEE 20th Int'l Symp. Personal Indoor and Mobile Radio Comm.*, pp. 2720-2724, Sept. 2009.
[23] H. Wang, L. Lightfoot, and T. Li, "On Phy-Layer Security of Cognitive Radio: Collaborative Sensing Under Malicious Attacks," *Proc. 44th Ann. Conf. Information Sciences and Systems*, pp. 1-6, Mar. 2010.
[24] L. Tong, Q. Zhao, and S. Adireddy, "Sensor Networks with Mobile Agents," *Proc. IEEE Military Comm. Conf.*, vol. 1, pp. 688-693, Oct. 2003.
[25] H. Urkowitz, "Energy Detection of Unknown Deterministic Signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523-531, Apr. 1967.
[26] M.R. Fellows, F.V. Fomin, D. Lokshtanov, F. Rosamond, S. Saurabh, and Y. Villanger, "Local Search: Is Brute-Force Avoidable?" *J. Computer and System Sciences*, vol. 78, no. 3, pp. 707-719, May 2012.
[27] M. Abdelhakim, L. Lightfoot, and T. Li, "Reliable Data Fusion in Wireless Sensor Networks under Byzantine Attacks," *Proc. IEEE Military Comm. Conf.*, Nov. 2011.
[28] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect Malicious Nodes in Collaborative Spectrum Sensing," *Proc. IEEE Global Telecomm. Conf.*, pp. 1-6, 2009.
[29] Y.L. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, pp. 305-317, Feb. 2006.
[30] A. Ghasemi and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," *Proc. First IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Networks*, pp. 131-136, 2005.

Mai Abdelhakim received the BSc and MSc degrees in communications engineering from Cairo University in 2006 and 2009, respectively. She is currently working toward the PhD degree in electrical and computer engineering at Michigan State University, on leave from her post as an assistant lecturer at the Egyptian National Center for Radiation Research and Technology. In 2006, she joined SySDSoft Inc. (currently Intel Mobile Communications) as an embedded software engineer. Then, she was a teaching assistant at the German University in Cairo and as a research assistant at the Center for Wireless Studies at Cairo University in 2007 and 2008, respectively. Her current research focuses on secure communications in sensor networks and high-speed wireless networks.

Leonard E. Lightfoot received the BS degree in computer engineering from Xavier University of Louisiana, New Orleans, LA in 2004 and the MS and PhD degrees in electrical engineering from Michigan State University, East Lansing, MI in 2006 and 2010, respectively. Currently, he is an in-house researcher for the Air Force Research Laboratory (AFRL), Wright-Patterson Air Force Base, OH. His research interest includes distributed sensor networks, radar communication systems, and network security.



Jian Ren received the BS and MS degrees both in mathematics from Shaanxi Normal University, and the PhD degree in EE from Xidian University, China. He is an associate professor in the Department of ECE at Michigan State University. He was the leading secure architect at Avaya Lab, Bell Lab and Racal Datacom in security architecture and solution development. His current research interests include cryptography, network security, energy efficient sensor network security protocol design, privacy-preserving communications, and cognitive networks. He received the US National Science Foundation Faculty Early Career Development (CAREER) award in 2009. He is a senior member of the IEEE.

Tongtong Li received the PhD degree in electrical engineering in 2000 from Auburn University. From 2000 to 2002, she was with Bell Labs, and had been working on the design and implementation of 3G and 4G systems. Since 2002, she has been with Michigan State University, where she is currently an associate professor. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory and statistical signal processing. She received the National Science Foundation (NSF) CAREER Award (2008) for her research on efficient and reliable wireless communications. She served as an associate editor for *IEEE Signal Processing Letters* from 2007 to 2009, and an Editorial Board member for *EURASIP Journal Wireless Communications and Networking* from 2004 to 2011. She is currently serving as the associate editor for *IEEE Transactions on Signal processing*.