ATTACK DETECTORS FOR DATA AGGREGATION IN CLUSTERED SENSOR NETWORKS

Roberto López-Valcarce and Daniel Romero

Department of Signal Theory and Communications, University of Vigo (Spain)

ABSTRACT

Among many security threats to sensor networks, compromised sensing is particularly challenging due to the fact that it cannot be addressed by standard authentication approaches. We consider a clustered scenario for data aggregation in which an attacker injects a disturbance in sensor readings. Casting the problem in an estimation framework, we systematically apply the Generalized Likelihood Ratio approach to derive attack detectors. The analysis under different attacks reveals that detectors based on similarity of means across clusters are suboptimal, with Bartlett's test for homoscedasticity constituting a good candidate when lacking a priori knowledge of the variance of the underlying distribution.

Index Terms— resilient data aggregation, attack detection, sensor networks.

1. INTRODUCTION

Sensor networks typically consist of a large number of low-cost sensor nodes measuring some physical phenomena and reporting their readings to a fusion center (FC) [1, 2]. As the overall data volume may be large, it is common to adopt clustered topologies in which cluster heads (CH) aggregate individual readings into compact reports sent to the FC, which in turn computes a global aggregated value. The average, count, min and max are typical aggregation functions [3, 4].

Security has long been recognized as a major challenge: sensor networks are susceptible to a variety of attacks such as physical tampering, node capture, denial of service, eavesdropping, etc. [5, 6]. In particular, sensor readings may be compromised before they reach a CH if an attacker alters the contents of data packets after capturing a node, or modifies the environmental parameters around some sensors; the latter need not be hard to achieve and does not require node capture. The effect of such malicious attacks (which cannot be detected by standard cryptographic means) on data aggregation was originally posed as an estimation problem and analyzed in [7], concluding that typical aggregation functions are very sensitive: the adversary can inflict very large distortion in the global aggregated value by compromising just a few nodes. Resilient aggregation functions based on robust statistics [8] were advocated in [7] as a means of defense, e.g. replacing the average by the sample median at the FC. In this way, robustness is achieved at the price of some performance loss. For example, in the absence of an attack, and assuming independent and identically distributed (i.i.d.) observations, the asymptotic Mean Squared Error (MSE) degradation when estimating the mean of the underlying distribution by using the sample median rather than the average is of 4.8 and 2 dB with uniform and Gaussian data, respectively [9].

Alternatively, it may be desirable to actually *detect* whether an attack is taking place, implementing mechanisms for this task in an initial step. Then, the usual aggregation function is applied if no attack is detected, as initially suggested in [10] and further developed in [11–14]; when an attack is declared, the FC may fall back on some resilient aggregation function as in [7]. In this way, the adversary faces a tradeoff between *distortion* and *detectability*.

We analyze different choices for attack detectors in this scenario. Following [7], we adopt an estimation viewpoint, regarding the average as a Maximum Likelihood estimator (MLE) for a Gaussian model. Attack detection is then posed as a hypothesis test at the FC based on local values aggregated at CHs. Adopting the Generalized Likelihood Ratio Test (GLRT) framework, previous ad hoc schemes [10–13] can be derived in this more rigorous way. Among these, some require a priori knowledge of the variance of the underlying distribution, whereas some others have poor performance. The GLRT approach also leads to other detectors not previously proposed in this context, such as Bartlett's test for homoscedasticity, which results in a better tradeoff in terms of a priori knowledge and attack detection performance.

2. SYSTEM MODEL

As in [7], we cast the data aggregation problem in an estimation theory framework. Consider a network of n sensors, divided into c clusters with n_i nodes each ($n = \sum_{i=1}^{c} n_i$). Sensor j in cluster i, denoted S_{ij}, acquires a measurement $x_{ij} \in \mathbb{R}$ and sends it to the corresponding cluster head CH_i, $i = 1, \ldots, c$, which appropriately aggregates the collected data and reports to an FC. The FC computes a global value summarizing the readings of all n sensors in the network, with the goal of estimating the value of an unknown parameter of

Supported by the Spanish Government and the European Regional Development Fund (ERDF) (projects TACTICA, COMPASS (TEC2013-47020-C2-1-R) and FPU Grant AP2010-0149) and by the Galician Regional Government and ERDF (projects GRC2013/009, R2014/037 and AtlantTIC).

interest θ of the physical environment. Thus, x_{ij} is modeled as a random variable whose distribution depends on θ. In particular we assume that, in the absence of attacks, the x_{ij} are i.i.d. and follow a normal distribution with mean θ and variance σ^2, denoted $N(\theta, \sigma^2)$. In that case, the MLE of θ is the (global) sample mean:

$$\hat{\theta} = \hat{\mu}_0 \triangleq \frac{1}{n} \sum_{i=1}^{c} \sum_{j=1}^{n_i} x_{ij} = \sum_{i=1}^{c} \frac{n_i}{n} \underbrace{\left(\frac{1}{n_i} \sum_{j=1}^{n_i} x_{ij} \right)}_{\triangleq \hat{\mu}_i}. \quad (1)$$

In (1), $\hat{\mu}_i$ is the *local* sample mean at cluster i. Thus, in this benign scenario, it suffices for each CH_i to send $(n_i, \hat{\mu}_i)$ to the FC, which in turn computes (1) as a weighted average.

Threat model. We assume a *myopic adversary* [7] which is able to observe and alter the readings of a subset $\mathcal{K}$ of sensors ($|\mathcal{K}| = k \ll n$), not all necessarily in the same cluster, and selected before the attack. The cluster heads and their communication links to the FC are assumed secure, so that the adversary cannot modify local computations at the CH_i's or their reports. Sensor readings can therefore be written as

$$x_{ij} = \tilde{x}_{ij} + z_{ij}, \quad (2)$$

where z_{ij} is an attacker-injected disturbance (therefore $z_{ij} = 0$ if $\mathrm{S}_{ij} \notin \mathcal{K}$), whereas the 'clean' values $\tilde{x}_{ij} = \theta + e_{ij}$ are i.i.d. with $e_{ij} \sim N(0, \sigma^2)$.

If the attack goes unnoticed, the estimation performance of (1) will deteriorate. This can be quantified in terms of the MSE *misadjustment,* defined as

$$\mathcal{M} \triangleq \frac{\mathrm{MSE}_{\text{attack}} - \mathrm{MSE}_{\text{no attack}}}{\mathrm{MSE}_{\text{no attack}}}, \quad (3)$$

where $\mathrm{MSE}_{\text{no attack}} = E\{(\theta - \hat{\theta})^2 \,|\, z_{ij} = 0 \,\forall\, i, j\} = \frac{\sigma^2}{n}$. Let $\tilde{\boldsymbol{x}}_c$, $\boldsymbol{e}_c$ and $\boldsymbol{z} \in \mathbb{R}^k$ comprise respectively the values of $\tilde{x}_{ij}$, e_{ij} and z_{ij} for sensors in set $\mathcal{K}$. It is readily checked that

$$\mathcal{M} = \frac{1}{n\sigma^2} \left[\mathbf{1}^T \boldsymbol{K}_{zz} \mathbf{1} + 2 \cdot \mathbf{1}^T \boldsymbol{K}_{ez} \mathbf{1} \right], \quad (4)$$

with $\boldsymbol{K}_{zz} \triangleq E\{\boldsymbol{z}\boldsymbol{z}^T\}$, $\boldsymbol{K}_{ez} \triangleq E\{\boldsymbol{e}_c \boldsymbol{z}^T\}$, and $\mathbf{1} \in \mathbb{R}^k$ the all-ones vector. Thus, the attacker is able to degrade performance by increasing the correlation of the injected disturbance (first term in (4)), and/or its cross-correlation with measurement noise (second term). Depending on the setting, the adversary may only have the ability to inject disturbances $\boldsymbol{z}$ in the compromised nodes *without* being able to observe the corresponding 'clean' values $\tilde{\boldsymbol{x}}_c$; in that case, $\boldsymbol{e}_c$, $\boldsymbol{z}$ are necessarily statistically independent and $\boldsymbol{K}_{ez} = \mathbf{0}$. This was the case considered in [10–13], which constrained $\boldsymbol{z} = \eta \mathbf{1}_k$, with η a constant. On the other hand, if the adversary can observe the sensor readings $\tilde{\boldsymbol{x}}_c$ of the k captured nodes[1], he may synthesize the injected disturbance $\boldsymbol{z}$ as a function of those readings.

[1] We assume that the adversary doe not have access to the readings of sensors not in set $\mathcal{K}$.

3. ATTACK DETECTORS: A GLRT APPROACH

In the absence of attacks, the fact that $x_{ij} \sim N(\theta, \sigma^2)\ \forall i, j$ implies uniformity of the mean (μ_i) and variance (σ_i^2) of the data across clusters: $\mu_i = \theta$ and $\sigma_i^2 = \sigma^2\ \forall i$. Based on this observation, different attack detectors can be devised.

3.1. Mean-based Detectors

If disparity of the means is considered as an indicator of the presence of an attack, an hypothesis test can be posed as:

$$\mathcal{H}_0 : \mu_1 = \cdots = \mu_c; \qquad \mathcal{H}_1 : \text{not all } \mu_i \text{ are equal}, \quad (5)$$

with μ_i the true mean of data from cluster i. Assuming a Gaussian model under both hypotheses, different tests result depending on knowledge about σ^2. An attack is declared if the corresponding statistic is larger than some threshold.

Common known variance. Assuming the variance σ^2 is the same under both hypotheses, the GLRT statistic is

$$L_G(\boldsymbol{x}) = \frac{\max\limits_{\{\mu_i\}} \prod_{i=1}^{c} (2\pi\sigma^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu_i \mathbf{1}\|^2}{2\sigma^2}}}{\max\limits_{\mu} \prod_{i=1}^{c} (2\pi\sigma^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu \mathbf{1}\|^2}{2\sigma^2}}}, \quad (6)$$

with $\boldsymbol{x}_i \triangleq [\, x_{i1} \ \cdots \ x_{in_i} \,]^T$. This is readily seen to yield

$$2 \log L_G(\boldsymbol{x}) = \frac{1}{\sigma^2} \sum_{i=1}^{c} n_i (\hat{\mu}_i - \hat{\mu}_0)^2, \quad (7)$$

with $\hat{\mu}_0$ and $\hat{\mu}_i$ as in (1). For clusters with equal sizes ($n_1 = \cdots = n_c = \frac{n}{c}$), this test was proposed in an ad hoc manner in [10] (for $c = 2$)[2] and [12, Sec. III-A] (for general c).

By Cochran's theorem [15], (7) follows a χ^2_{c-1} distribution under $\mathcal{H}_0$. This holds true even if the $\{x_{ij}\}$ are not Gaussian, provided that the n_i's are sufficiently large so that $\{\hat{\mu}_i\}$ are approximately Gaussian by the Central Limit Theorem, and allows to set the threshold for a given probability of false alarm P_{FA} as long as σ^2 is known. Note that the FC can compute (7) directly from the $(n_i, \hat{\mu}_i)$ data sent from the CH_i's.

Common unknown variance. If σ^2 is regarded as a nuisance parameter under both hypotheses, the numerator and denominator in (6) must be maximized w.r.t. $\{\mu_1, \ldots, \mu_c, \sigma^2\}$ and $\{\mu, \sigma^2\}$ respectively, yielding the following test statistic:

$$2 \log L_G(\boldsymbol{x}) = n \log \left(1 + \frac{\sum_{i=1}^{c} \frac{n_i}{n} (\hat{\mu}_i - \hat{\mu}_0)^2}{\sum_{i=1}^{c} \frac{n_i}{n} \hat{\sigma}_i^2} \right), \quad (8)$$

where $\hat{\sigma}_i^2$ denotes the *local* sample variance at cluster i:

$$\hat{\sigma}_i^2 \triangleq \frac{1}{n_i} \sum_{j=1}^{n_i} (x_{ij} - \hat{\mu}_i)^2. \quad (9)$$

[2] For $c = 2$ and $n_1 = n_2 = \frac{n}{2}$, (7) can be written as $2 \log L_G(\boldsymbol{x}) = \frac{n}{4\sigma^2} (\hat{\mu}_1 - \hat{\mu}_2)^2$, which is the "Split & Check" detector from [10].

Now the CH_i's must transmit $(n_i, \hat{\mu}_i, \hat{\sigma}_i^2)$ to the FC. This is the case as well for all detectors in the sequel.

Note that (8) is equivalent to the "analysis of variance" (ANOVA) F-test statistic [16, 17]

$$F = \frac{n-c}{c-1} \frac{\sum_{i=1}^{c} n_i(\hat{\mu}_i - \hat{\mu}_0)^2}{\sum_{i=1}^{c} n_i \hat{\sigma}_i^2}, \tag{10}$$

which, under $\mathcal{H}_0$, follows an F distribution with $c-1$ and $n-c$ degrees of freedom. For $c = 2$, the F-test reduces to Student's t-test [17]. In [13], such t-test was proposed for detecting attacks concentrated in a given cluster, by combining data from all remaining clusters in a single "supercluster".

3.2. Variance-Based Detectors

A different approach to attack detection is to test for equality of variances across different clusters (homoscedasticity), i.e.,

$$\mathcal{H}_0 : \sigma_1^2 = \cdots = \sigma_c^2; \qquad \mathcal{H}_1 : \text{not all } \sigma_i^2 \text{ are equal}, \tag{11}$$

whereas the means $\{\mu_i\}$ are regarded as nuisance parameters.

Known variance under $\mathcal{H}_0$. If under $\mathcal{H}_0$ the common variance is known to be σ^2, the GLRT statistic becomes

$$L_G(\boldsymbol{x}) = \frac{\max\limits_{\{\mu_i, \sigma_i^2\}} \prod_{i=1}^{c} (2\pi\sigma_i^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu_i \mathbf{1}\|^2}{2\sigma_i^2}}}{\max\limits_{\{\mu_i\}} \prod_{i=1}^{c} (2\pi\sigma^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu_i \mathbf{1}\|^2}{2\sigma^2}}}, \tag{12}$$

resulting in

$$2\log L_G(\boldsymbol{x}) = \sum_{i=1}^{c} n_i \left(\frac{\hat{\sigma}_i^2}{\sigma^2} - \log \frac{\hat{\sigma}_i^2}{\sigma^2} - 1 \right), \tag{13}$$

which, under $\mathcal{H}_0$ and for large n, is χ_c^2-distributed. The first term in (13) corresponds to the ad hoc test proposed in [12, Sec. III-B], which follows a χ_{n-c}^2 distribution under $\mathcal{H}_0$:

$$T \triangleq \frac{1}{\sigma^2} \sum_{i=1}^{c} n_i \hat{\sigma}_i^2. \tag{14}$$

Unknown variance under $\mathcal{H}_0$. Regarding σ^2 as a nuisance parameter under $\mathcal{H}_0$, the denominator in (12) must be maximized w.r.t. $\{\mu_i\}$ and σ^2, yielding *Bartlett's test* [18]:

$$2\log L_G(\boldsymbol{x}) = n \log \frac{\sum_{j=1}^{c} \frac{n_j}{n} \hat{\sigma}_j^2}{\prod_{i=1}^{c} (\hat{\sigma}_i^2)^{\frac{n_i}{n}}}, \tag{15}$$

Under $\mathcal{H}_0$ and for large n, (15) is χ_{c-1}^2-distributed.

3.3. Mean and Variance-Based Detector

Testing for equality of means *and* variances simultaneously,

$$\mathcal{H}_0 : \quad (\mu_1, \sigma_1^2) = \cdots = (\mu_c, \sigma_c^2), \tag{16}$$

results in the GLRT statistic given by

$$L_G(\boldsymbol{x}) = \frac{\max\limits_{\{\mu_i, \sigma_i^2\}} \prod_{i=1}^{c} (2\pi\sigma_i^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu_i \mathbf{1}\|^2}{2\sigma_i^2}}}{\max\limits_{\{\mu, \sigma^2\}} \prod_{i=1}^{c} (2\pi\sigma^2)^{-\frac{n_i}{2}} \mathrm{e}^{-\frac{\|\boldsymbol{x}_i - \mu \mathbf{1}\|^2}{2\sigma^2}}}, \tag{17}$$

yielding $2\log L_G(\boldsymbol{x})$

$$= n \log \frac{\sum_{j=1}^{c} \frac{n_j}{n} \hat{\sigma}_j^2}{\prod_{i=1}^{c} (\hat{\sigma}_i^2)^{\frac{n_i}{n}}} + n \log \frac{\sum_{j=1}^{c} \frac{n_j}{n} (\hat{\mu}_j - \hat{\mu}_0)^2}{\prod_{i=1}^{c} (\hat{\sigma}_i^2)^{\frac{n_i}{n}}}, \tag{18}$$

which is $\chi_{2(c-1)}^2$-distributed under $\mathcal{H}_0$ and for large n. Note that the first term in (18) is Bartlett's test statistic (15).

4. NUMERICAL RESULTS

The detectors from Secs. 3.1-3.3 are studied under different kinds of attacks. The network has $n = 128$ sensor nodes in c clusters, $c \in \{2, 4, 8\}$, all of the same size $\frac{n}{c}$. The SNR is $\theta^2/\sigma^2 = 10$ dB, and for all detectors considered, the thresholds are set for $P_{\mathrm{FA}} = 0.05$. The attacker has control over $k = 5$ nodes and no knowledge of the network cluster structure; thus, at each Monte Carlo run, the k compromised nodes are chosen randomly and independently among the n network nodes. Three different attack types are considered:

- *Type A:* The injected disturbance values are i.i.d. with $z_{ij} \sim N(0, \delta^2)$ for $\mathrm{S}_{ij} \in \mathcal{K}$, and independent of sensor readings. Thus $\boldsymbol{K}_{zz} = \delta^2 \boldsymbol{I}_k$, $\boldsymbol{K}_{ez} = \mathbf{0}$ and $\mathcal{M} = \frac{k}{n} \frac{\delta^2}{\sigma^2}$.
- *Type B:* The disturbance is proportional to the sensor reading, i.e., $z_{ij} = a \cdot x_{ij}$ for $\mathrm{S}_{ij} \in \mathcal{K}$. This yields $\boldsymbol{K}_{zz} = a^2(\theta^2 \mathbf{1}\mathbf{1}^T + \sigma^2 \boldsymbol{I}_k)$, $\boldsymbol{K}_{ez} = a\sigma^2 \boldsymbol{I}_k$, so that $\mathcal{M} = a^2 \frac{k^2}{n} \frac{\theta^2}{\sigma^2} + (a^2 + 2a) \frac{k}{n} \approx a^2 \frac{k^2}{n} \frac{\theta^2}{\sigma^2}$ in high SNR.
- *Type C:* The disturbance is constant across compromised nodes: $z_{ij} = b \; \forall \mathrm{S}_{ij} \in \mathcal{K}$, with b a deterministic constant. Thus, $\boldsymbol{K}_{zz} = b^2 \mathbf{1}\mathbf{1}^T$, $\boldsymbol{K}_{ez} = \mathbf{0}$, and $\mathcal{M} = \frac{k^2}{n} \frac{b^2}{\sigma^2}$.

Results are shown in Fig. 1 for $c = 2$, 4, and 8 clusters. The following observations can be made:

1. The variance-based detectors (13) (GLRT for homoscedasticity) and (14) (Luo's χ^2 test [12]) consistently outperform the remaining schemes. However, they require knowledge of σ^2 to set the threshold for a given P_{FA}. If, e.g., the target is $P_{\mathrm{FA}} = 0.05$ and σ^2 is underestimated in just 1 dB, in this setting Luo's detector (14) yields $P_{\mathrm{FA}} \approx 0.56$, 0.5 and 0.4 for $c = 2$, 4 and 8 clusters, respectively.

2. The F-test (10) is not adequate for attack detection. To further illustrate this observation, suppose a single node, say S_{11}, is compromised ($k = 1$). In that case, it can be easily shown that, for large values of z_{11}^2, (10) becomes

$$F \approx \frac{n-c}{c-1} \frac{z_{11}^2 \frac{n-n_1}{n_1 n} + \sum_{i=1}^{c} n_i (\tilde{\mu}_i - \tilde{\mu}_0)^2}{z_{11}^2 \frac{n_1 - 1}{n_1} + \sum_{i=1}^{c} n_i \tilde{\sigma}_i^2}, \tag{19}$$

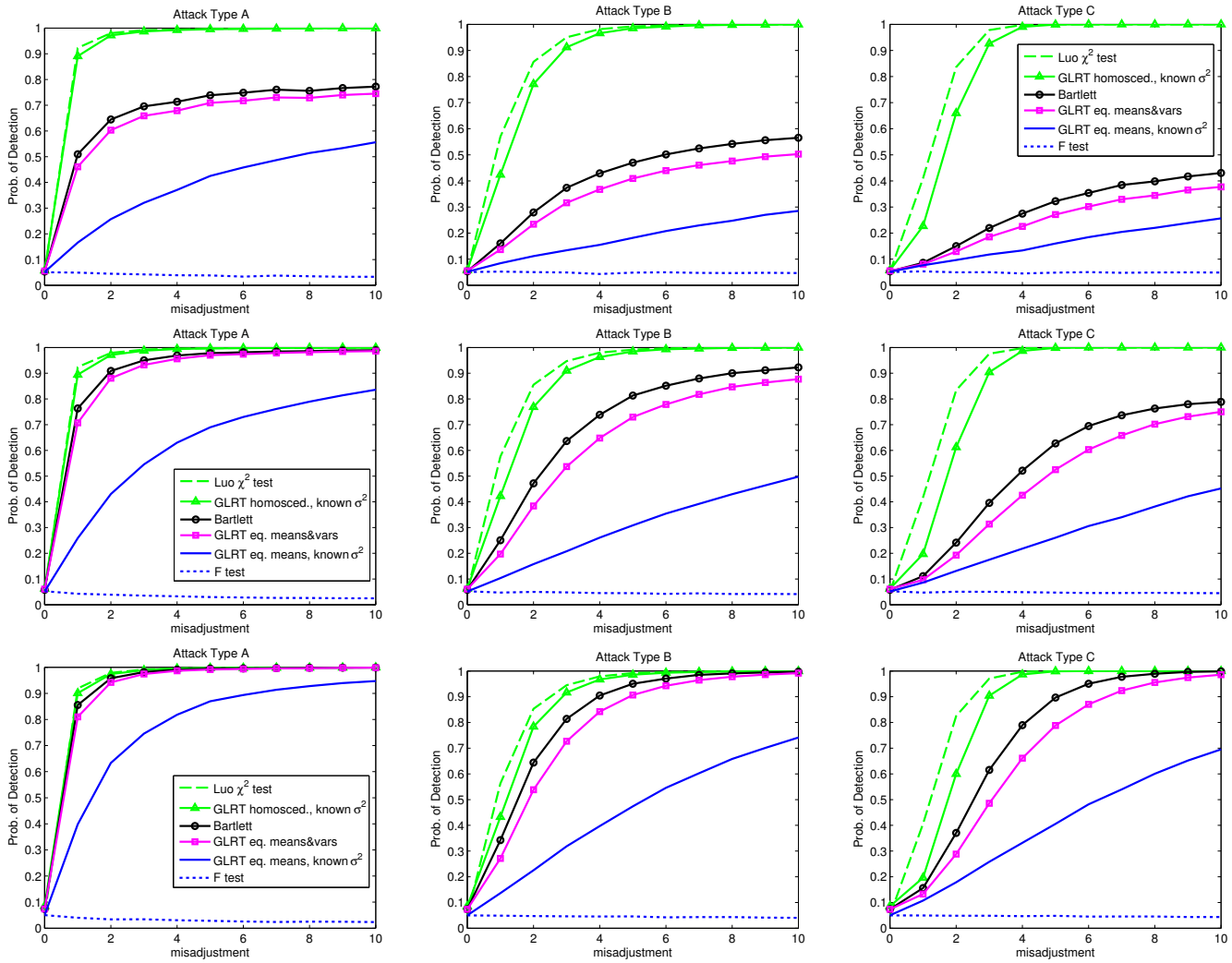

Fig. 1. Probability of detection ($P_{\rm D}$) vs. $\mathcal{M}$ for the considered detectors under different attack types. $P_{\rm FA} = 0.05$, network size $n = 128$, $k = 5$ compromised nodes. Top row: $c = 2$ clusters. Middle row: $c = 4$ clusters. Bottom row: $c = 8$ clusters.

where $\tilde{\mu}_i$, $\tilde{\sigma}_i^2$ are the values of $\hat{\mu}_i$, $\hat{\sigma}_i^2$ in the absence of attack ($z_{11} = 0$). From (19), $F \to \frac{(n-c)(n-n_1)}{(c-1)n(n_1-1)}$ as $z_{11}^2 \to \infty$. If, e.g., $n_1 = \frac{n}{c}$, then $F \to 1$, which will be below the detection threshold for practical $P_{\rm FA}$ values. Hence, the attacker can inflict an arbitrarily large distortion with a small probability of detection, even with a *single* compromised node.

3. In contrast with the F-test, the GLRT detector (7) (equality of means) [10, 12], is responsive to attacks, but it is outperformed by the remaining schemes. In addition, it requires knowledge of σ^2 in order to set the threshold.

4. Bartlett's test (15) outperforms the GLRT for equality of means and variances (18): the addition of the second term in (18) is seen to be detrimental. This term can be seen as a test for equality of means[3]. Thus, it is concluded that *equality of means across clusters is not a good attack detection criterion.* To see this, suppose that the adversary compromises k_i nodes in cluster i and launches a Type C attack. It can be easily shown that if $\frac{k_i}{n_i} = \frac{k}{n}$ $\forall i$, then the differences $\hat{\mu}_i - \hat{\mu}_0$ are unaltered by the attack. Due to this kind of events, for mean-based schemes $P_{\rm D}$ remains bounded away from 1 as the distortion becomes arbitrarily large, even when the compromised nodes are picked at random.

5. For all detectors considered, Type C attacks have more power (larger distortion for a given $P_{\rm D}$) than Type B attacks, which in turn have more power than Type A attacks.

6. Whereas detectors (13)-(14) remain insensitive to the number of clusters, the performance of detectors (7), (15) and (18) degrades with too few clusters. The explanation is as follows. Suppose the adversary captures exactly one node per cluster, launching a Type C attack. Then $\hat{\mu}_i = \tilde{\mu}_i + \frac{1}{n_i} b$, and

[3]Note the similarity of the second term in (18) with (10): the arithmetic mean of the sample variances is replaced by the geometric mean.

for large b^2, $\hat{\sigma}_i^2 \approx \tilde{\sigma}_i^2 + b^2 \frac{n_i - 1}{n_i^2}$, with $\tilde{\mu}_i$, $\tilde{\sigma}_i^2$ the sample means and variances, respectively, in the absence of attack. Since one can expect the $\tilde{\mu}_i$'s, and also the $\tilde{\sigma}_i^2$'s, to be close to each other, with equal-size clusters ($n_i = \frac{n}{c}\ \forall i$) so will the $\hat{\mu}_i$'s and $\hat{\sigma}_i^2$'s; and even more so as $|b|$ increases, since in that case $\hat{\mu}_i \to \frac{c}{n} b$ and $\hat{\sigma}_i^2 \to b^2 \frac{c}{n}(1 - \frac{c}{n})$, which are independent of i. Thus, the attack is likely to go undetected, *with arbitrarily large distortion*. This explains why some of the P_{D} curves of these detectors in Fig. 1 for $c = 2$ and $c = 4$ seem to saturate at a value less than 1. For $c > k$, this kind of event is no longer feasible and detection performance significantly improves.

5. CONCLUSIONS

We have systematically applied a GLRT approach to sensor attack detection, revealing a variety of tests. Some of them had been previously proposed in an ad hoc manner, and some others are novel in this context. It has been shown that exploiting uniformity of means across clusters is outperformed by homoscedasticity based schemes, with Bartlett's test achieving good performance as long as the number of clusters in the network is not too low, without requiring a priori knowledge about the variance of the underlying distribution. The power of different attack types has also been discussed.

Future work will address more sophisticated data models, including spatial correlation among sensor readings [14] and different parametric dependencies of the readings' pdf and the parameters of interest. Also, Bartlett's test is known to be sensitive to deviations from normality [17]. Levene's test [19] is a popular robust alternative in statistics, but since it is posed as an F-test on a transformed data set, it is not well suited to attack detection, similarly to the standar F-test (10).

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] P. Corke, T. Wark, R. Jurdak, Wen Hu, P. Valencia, and D. Moore, "Environmental wireless sensor networks," *Proc. IEEE*, vol. 98, no. 11, pp. 1903–1916, Nov. 2010.

[3] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring wireless sensor networks," in *IEEE Int. Workshop on Sensor Network Protocols and Applications (SNPA)*, 2003, pp. 139–148.

[4] R. Rajagopalan and P.K. Varshney, "Data aggregation techniques in sensor networks: a survey," *IEEE Commun. Surveys Tut.*, vol. 8, no. 4, pp. 48–63, 2006.

[5] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[6] Xiangqian Chen, K. Makki, Kang Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2nd quarter 2009.

[7] D. Wagner, "Resilient aggregation in sensor networks," in *ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, Oct. 2004.

[8] A.M. Zoubir, V. Koivunen, Y. Chakhchoukh, and M. Muma, "Robust estimation in signal processing," *IEEE Signal Process. Mag.*, vol. 29, no. 4, pp. 61–80, Jul. 2012.

[9] D. Williams, *Weighing the odds*, Cambridge Univ. Press, 2001.

[10] L. Buttyán, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in *IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOMW)*, 2006.

[11] Yong-Jian Luo, Xin Yang, and Xu Zhang, "An effective resilient data aggregation algorithm in wireless sensor networks," in *IEEE Int. Conf. Wireless Commun., Netw., Mobile Comput. (WiCom)*, 2007, pp. 2642–2645.

[12] Yong-Jian Luo, Yan-Dan Tao, Xu Zhang, Xin Yang, and Yin-Sheng Wu, "Two effective attack detection algorithms in wireless sensor networks," in *IEEE Int. Conf. Wireless Commun., Netw., Mobile Comput.*, 2008.

[13] Yong-Jian Luo, Xiao-Yong Ding, Gang Wu, and Guang-Dong Ding, "A novel attack detection algorithm based on t-distribution in wireless sensor networks," in *IEEE Int. Conf. Wireless Commun., Netw., Mobile Comput. (WiCom)*, 2009.

[14] L. Buttyán, P. Schaffer, and I. Vajda, "CORA: Correlation-based resilient aggregation in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1035–1050, Aug. 2009.

[15] W. G. Cochran, "The distribution of quadratic forms in a normal system, with applications to the analysis of covariance," *Proc. Cambridge Philos. Soc.*, vol. 30, pp. 178–191, 1934.

[16] H. Scheffé, *The Analysis of Variance*, Wiley, 1959.

[17] H. Sahai and M.I. Ageel, *The Analysis of Variance: fixed, random and mixed models*, Springer, 2000.

[18] M. S. Bartlett, "Properties of sufficiency and statistical tests," *Proc. Royal Soc. London*, vol. 160A, pp. 268–282, 1937.

[19] H. Levene, "Robust tests for equality of variances," in *Contributions to Probability and Statistics*, I. Olkin, S.G. Ghurye, W. Hoeffding, W.G. Madow, and H.B. Mann, Eds., pp. 278–292. Stanford Univ. Press, Stanford, CA, 1960.