Sensor Source Location Privacy based on Random Perturbations

Uthaiwan Srimongkolpitak
School of Engineering
The Catholic University of America
Washington DC, USA
E-mail: 95srimongkol@cardinalmail.cua.edu

Yi Yang
School of Engineering
The Catholic University of America
Washington DC, USA
E-mail: yangy@cua.edu

***Abstract*—Sensor source location privacy, which means to protect source sensors' locations of network traffic, is an emerging topic in wireless sensor networks, because it cannot be fully addressed by traditional cryptographic mechanisms, such as encryption and authentication. Current source location privacy schemes, assuming either a local attack model or a global attack model, have limitations. For example, schemes under a global attack model are subject to a so called '01' attack. Targeting on solving this attack under a global attack model, we propose two perturbation schemes, one based on Uniform distribution and the other based on Gaussian distribution. We analyze the security properties of these two schemes. We also simulate them and compare them with previous schemes, with the results showing that the proposed perturbation schemes can improve the source location privacy significantly.**

***Index Terms*—Source Location Privacy, Wireless Sensor Networks, Random Perturbations, Uniform Distribution, Gaussian Distribution.**

I. Introduction

Sensors are small devices that can collect data, e.g., acoustic, temperature, and vibration, from the environment. To fulfil their goals, sensors have three salient features. First, they have small sizes, so they are widely used in ubiquitous/pervasive computing, to complete tasks without being noticed by people, especially by those enemies in a battlefield environment. Second, they operate under very limited resources, such as simple processor, small storage, and scarce power. Therefore, only lightweight operations are affordable by sensors. Third, sensors communicate with each other through simple radio devices and normally in an open/broadcast manner, so it is easy for the attacker to overhear message transmissions among sensors. Overall, sensors radically change the way in which people observe and interact with the environment.

A large quantity (e.g., hundreds or even thousands) of sensors communicating with each other consist of a Wireless Sensor Network (WSN). WSNs are widely used for essential military missions and civilian tasks, such as battlefield surveillance, seismic monitoring of buildings, and personal health maintenance. However, WSNs are also susceptible to a myriad of attacks [1], because they normally operate in an unattended, harsh, and/or hostile environment.

Traditional research in WSNs focuses on solving such security issues as key establishment and management [2], [3], [4], [5], [6], [7], data encryption/decryption, and message integrity/source authentication [8]. Most of them could be solved by techniques such as applied cryptography. Recently, privacy preservation, which cannot be fully addressed by encryption and authentication, has drawn a lot of attention from researchers [9], [10], [11], [12], [13], [14], [15], [16], [17], [18]. One way to categorize privacy preservation is to divide it into protecting either sources' or receiver's location. Since the receiver, i.e., the base station, is normally protected by tamper proof mechanisms because of its importance, our focus is source location privacy, which means to protect the source nodes' locations of the network traffic.

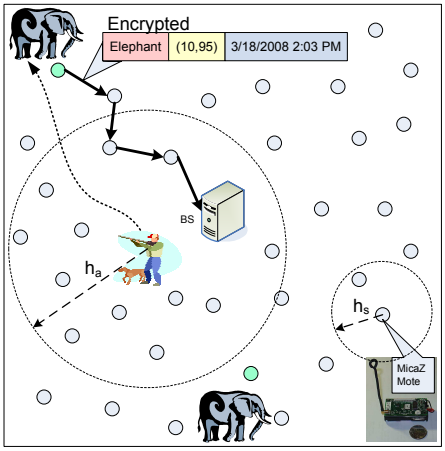

Fig. 1. An application of sensor networks for animal monitoring, in which h_a is the hearing range of the attacker and h_s is the hearing range of regular sensors.

If a message is transmitted from source to destination, no matter how strong the key and algorithm to encrypt the data are, the location of the source is disclosed to the observer by traffic analysis. As shown in Figure 1, in an asset monitoring network to protect the elephant, the attacker can thus locate the elephant and capture them. In a battlefield scenario, the communication between soldiers and their surrounding sensors could reveal the positions of the soldiers, putting them in great danger as the opposing force, by monitoring sensor network traffic, may locate the soldiers and accurately attack them. Therefore, source location privacy is a challenging issue.

COLLABORATECOM 2012, October 14-17, Pittsburgh, United States

DOI 10.4108/icst.collaboratecom.2012.250621

Although there are existing solutions in literature, there are still limitations in them. The current source privacy preservation techniques assume either a local or global attack model. In a local attack model, the attacker has a hearing range comparable to that of regular sensors. In this case, when the attacker's hearing range increases to more than three times of regular sensors, the asset capture likelihood by phantom routing significantly increases to 97% [12].

On the other hand, in a global attack model, the researchers directly consider an attacker with a hearing range covering the entire network, by either deploying his own malicious network or employing a powerful site surveillance device [15]. These schemes are subject to a so called '01' test from the attacker [19], because a time interval of real message is normally smaller than the population mean, followed by a recovery time interval of dummy message that is larger than the population mean. If over time the attacker accumulates an accurate population mean of message time intervals, then he can identify all these '01' patterns of time intervals (we denote a time interval smaller than mean as '0' and a time interval larger than mean as '1'). Thus, he has a high chance to derive that the '0's in these patterns are likely to be real message time intervals.

Targeting on solving this '01' attack in previous schemes, we propose two perturbation schemes, one based on Uniform distribution and the other based on Gaussian distribution. By adding perturbations to the message time intervals, the sample mean calculated by the attacker deviates from the true (or population) mean, which makes the '01' patterns obscure and lowers the attacker's detection capability. We analyze the security properties of these two schemes. We also simulate them and compare them with previous schemes, with results to show that these two perturbation schemes could improve the source location privacy significantly.

The rest of the paper is organized as follows. We first talk about the background knowledge of previous work [15] and '01' attack in Section II. Then, we formalize the system model in Section III. After that, we propose the two perturbation schemes in Section IV before security analysis in Section V. The performance evaluation is in Section VI. Finally, we briefly discuss the related work in Section VII and conclude our paper in Section VIII.

II. Background

In this section, we cover some background knowledge on previous work and try to answer the following questions: why do we care about message time intervals? What are sample mean and population mean of message time intervals? Why does the previous work suffer from '01' attack? What do '0' and '1' mean in this attack?

A. Previous Work

We focus on the most important previous work, which is [15]. This work considers a global attack model, which means the attacker has a global view of all the network traffic. Under such a strong attack model, we have to introduce extra message overhead (i.e., dummy messages) with the same format to cover real messages. By observing message formats, the attacker cannot differentiate real and dummy messages.

The simplest scheme with perfect privacy under this condition is a constant-rate scheme, in which all the nodes send out messages following the same rate. When there is a real event, real source postpones the message transmission to the next time interval. However, in this scheme, there is a difficulty in determining message transmission rate: when this rate is too high, there will be much overhead introduced from dummy messages; otherwise, if this rate is too low, there will be high latency in real message transmissions. Therefore, there is a tradeoff among privacy, overhead, and latency inherently.

The main purpose of FitProbRate scheme in [15] is to reduce real event report latency by relaxing perfect privacy requirement. In FitProbRate scheme, every nodes send out messages following a probabilistic rate, i.e., an exponential distribution, which provides flexibility to reduce real message latency. Real sources use goodness of fit test to generate small real message time intervals with the same distribution. However, under this condition, if there are continuous real messages and/or real message rate is high, then the mean of message time intervals will tend to be small. Hence, real message time intervals normally are followed by relatively large dummy message time intervals to recover the mean.

Note that here the mean of the attacker refers to the attacker's sample mean, which is limited by the attacker's window size, due to his finite computation and storage resources. The attacker's population mean is the mean of sample means.

B. '01' Attack

The previous work [15] suffers from a so called '01' test from the attacker [19]. Over time, the attacker may accumulate a population mean of all the observed message time intervals. If his population mean is accurate, he can identify all the message time intervals smaller than this mean (denoted as '0's) and all the message time intervals larger than this mean (denoted as '1's). Furthermore, he may tend to find that message time intervals smaller than this mean have a higher chance of coming from real sources. An intuitive way for the attacker to identify real messages is to find out all the '01' patterns of message time intervals and derive '0's in these patterns are likely from real messages.

III. System Models

Next, we introduce our network model as well as adversary model.

A. Network Model

We consider that n sensor nodes are randomly distributed in the deployment area. There are $n'(0 < n' < n)$ out of n nodes detecting real events and sending real messages simultaneously. Once a real event is detected, real messages containing real event related information, such as event type, location, and time will be sent from the source to the base station. Dummy messages are generated to cover these real

messages. All messages are encrypted and of the same format. Base station resides in a fixed location in the network, e.g., at the center.

B. Adversary Model

Since all the messages are scrambled and appear random to the attacker, the attacker has to try to identify real messages from their time intervals because real sources tend to send out real messages as soon as possible to reduce the latency. In our attack model, the attacker has a hearing range h_a, which is multiple times larger than that of the regular sensors h_s(i.e., $3h_s < h_a \leq r$, where r is network radius), e.g., a laptop-class attacking device with more powerful but limited hearing capabilities. We assume that maximally the attacker can observe and analyze w message time intervals altogether, i.e., the attacker's window size is $w \geq 0$. We differentiate sensor's transmission range (t_s) and hearing range (h_s), i.e., t_s might not equal to h_s. The attacker might compromise a small fraction of sensor nodes to stop their normal operations and obtain their security credentials. Like other papers in the same area [15], [14], [13], we assume that the base station cannot be compromised.

IV. Proposed Schemes

As introduced formerly, the previous schemes under a global attack model are subject to a so called '01' attack. Targeting on solving this attack, we present our two source location privacy schemes based on random perturbations: one based on Uniform distribution and the other based on Gaussian distribution.

These two schemes work because based on random perturbations the sample mean calculated by the attacker becomes inaccurate, which means it deviates from the true or population mean. In this way, the attacker cannot accurately identify all the '01' patterns, and this decreases the attacker's detection capability for real message time intervals significantly.

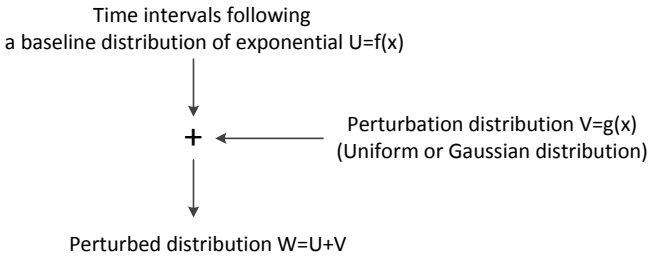

Fig. 2. Adding perturbations into message time intervals.

A. A Scheme based on Uniform Distribution

Similar to [15], the baseline of message time intervals follows an exponential distribution, because according to its probability density function, a traffic generator following an exponential distribution tends to generate small time intervals. Our basic idea is to add random perturbations to each individual time interval following an exponential distribution. As shown in Figure 2, every time interval will follow the probabilistic distribution of $U + V$ instead of only U, where U is the exponential distribution and V is the perturbation distribution.

The common perturbations normally follow two different distributions. The first one is a Uniform distribution with 0 as mean and range is $[-a, +a]$. The second perturbation could be a Gaussian distribution, which will be discussed in the next section.

Every time a real message comes, a small interval with maximum negative perturbation could be assigned, e.g., $-a$ in Uniform distribution; we still need to guarantee that the time intervals from real messages are positive and small. The technique to implement this perturbation is presented in Algorithm 1.

Algorithm 1 Perturbation based on Uniform Distribution

Input: uniform distribution in range $[-a, a]$; rate r of real event; duration d of real event; mean μ of exponential distribution;

Output: m message time intervals $\lambda_i (0 \leq i \leq m-1)$ including time intervals of real event messages;

Procedure:

```
1: val = round(1/r);
2: for i = 0 to m − 1 do
3:    if rem(i, val)=0 then
4:       for j = 0 to d − 1 do
5:          λ_ij = exprnd(μ)-a;{maximally negative perturbations}
6:          while λ_ij <= 0 do
7:             λ_ij = exprnd(μ)-a;{time intervals should be positive}
8:          end while
9:       end for
10:   else
11:      λ_i = exprnd(μ)+unifrnd((-1)×a, a);{regular perturbations following uniform distribution}
12:      while λ_i <= 0 do
13:         λ_i = exprnd(μ)+unifrnd((-1)×a, a);{time intervals should be positive}
14:      end while
15:   end if
16: end for
```

B. A Scheme based on Gaussian Distribution

The second perturbation could be a Gaussian distribution with 0 as mean and standard deviation σ. Every time a real message comes, a small interval with maximum negative perturbation could be assigned, e.g., $-\sigma$, $-2 \times \sigma$, or even $-3 \times \sigma$ in Gaussian distribution. We still need to guarantee that the time intervals from real messages are positive and small. The details of implementation are presented in Algorithm 2.

In order to guarantee that the generated time intervals are positive, the basic idea of our algorithm is that every time when we generate a random time interval we check whether it is positive or not; if not, we repeat this process until every random time interval is positive. Since the operations of random number generator are simple, we can find positive random values very fast.

Algorithm 2 Perturbation based on Gaussian Distribution

Input: standard deviations σ; rate r of real event; duration d of real event; mean μ of exponential distribution;
Output: m perturbed time intervals $\lambda_i (0 \leq i \leq m-1)$;
Procedure:

```
val = round(1/r);
for i = 0 to m − 1 do
    if rem(i, val)=0 then
        for j = 0 to d − 1 do
            λ_ij = exprnd(μ)+b; {maximally negative perturbation when b is −σ, −2 × σ, or −3 × σ}
            while λ_ij <= 0 do
                λ_ij = exprnd(μ)+b; {time intervals should be positive when b is −σ, −2 × σ, or −3 × σ}
            end while
        end for
    else
        λ_i = exprnd(μ)+normrnd(0, σ);
        while λ_i <= 0 do
            λ_i = exprnd(μ)+normrnd(0, σ); {time intervals should be positive}
        end while
    end if
end for
```

V. Security Analysis

In this section, we analyze the security properties of previous work [15] and the proposed schemes. More specifically, we analyze the probability for '01' patterns to occur for all these schemes.

First, let us take a look at the probability for '01' patterns to appear in FitProbRate scheme [15]. Suppose m is the total number of messages and r is real message rate. There are two situations for '01' patterns to occur: if there are real events, then the probability for '01' pattern to appear is 1; otherwise, if there are no real events, then the probability for '01' pattern to appear is $1/4$, because the probability for two continuous messages to be the pattern of '00', '01', '10', and '11' are all equal. Hence, according to Total Probability Formula and Classical Probability Model, the probability $p(x_1)$ for '01' patterns to appear in FitProbRate scheme is as follows:

$$p(x_1) = \frac{m \times r + (m - m \times r) \times \frac{1}{4}}{m-1} = \frac{3 \times m \times r + m}{4 \times (m-1)}$$

when m is large

$$\approx \frac{3}{4} \times r + \frac{1}{4}. \quad (1)$$

Then, let us take a look at the probability for '01' patterns to appear in our schemes. The probability $p(x_2)$ for '01' pattern to appear is $1/4$, because due to our random perturbations the probability for two continuous messages to be the pattern of '00', '01', '10', and '11' are all equal, i.e.,

$$p(x_2) = \frac{1}{4} < p(x_1), \quad (2)$$

since $r > 0$. This means that the probability for '01' patterns to occur in our schemes is smaller than that in the FitProbRate scheme and the actual difference depends on the real message rate.

We will use simulations in Section VI-C1 to validate our analytical results. The probability for '01' patterns to appear in our schemes is close to $1/4$, which is the probability for any random patterns of two continuous message intervals to appear. This means that by perturbations the '01' patterns of real message time intervals are hidden well in a large quantity of dummy message time intervals. Also, this probability is smaller than that in the FitProbRate scheme, which means that our perturbation schemes can reduce the probability for '01' patterns to occur from a relatively large value (though the difference depends on the real message rate) to a value for random patterns, so that the attacker cannot gain anything from purely identifying '01' patterns.

VI. Performance Evaluation

In this section, we first introduce the setup of our simulation and the evaluation metrics, then we present our simulation results.

A. Simulation settings

In our simulation settings, there are 100 nodes randomly distributed in the deployment area. Out of them, there are 5 real sources detecting real events. By default, a real event lasts for 5 messages (i.e., duration $\lambda = 5$). We choose the rates of real event to be 0.01, 0.02, 0.04, 0.05, 0.1. The mean of the exponential distribution is 10. The perturbation parameters (a) in Uniform distribution and (σ) in Gaussian distribution are 5. For the attacker, his window size is 1000 by default. The attacker uses one-sample Kolmogorov-Smirnov test as his goodness of fit test and the significance level (α) in his statistic test is 5%.

B. Simulation metrics

Here in our simulation a detection is defined as "a '01' pattern has been identified". Then, detection rate is formulated as follows:

Definition 1: Suppose the number of detected *'01' patterns caused by real messages is denoted as t and the* actual total *number of '01' patterns caused by real messages in the traffic is denoted as $t'(t \leq t')$, then the detection rate of attacker is defined as:*

$$detection\ rate = t/t'.$$

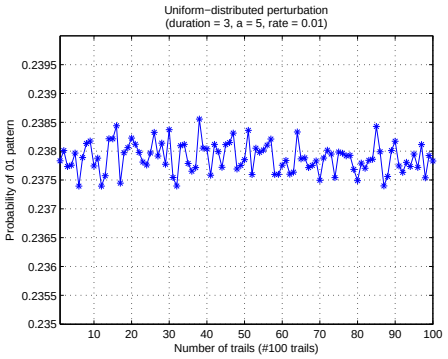

Fig. 3. Validating analysis on Uniform distribution

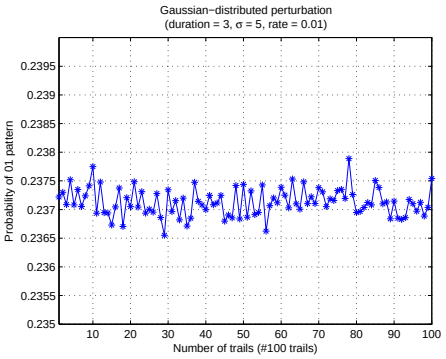

Fig. 4. Validating analysis on Gaussian distribution

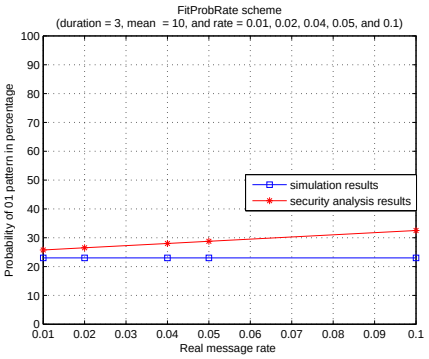

Fig. 5. Validating analysis on FitProbRate scheme

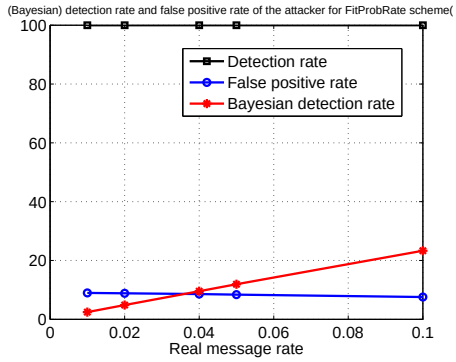

Fig. 6. The FitProbRate scheme.

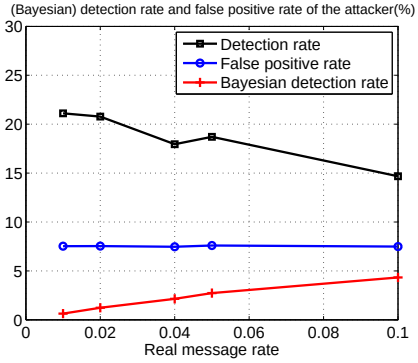

Fig. 7. Uniform perturbations.

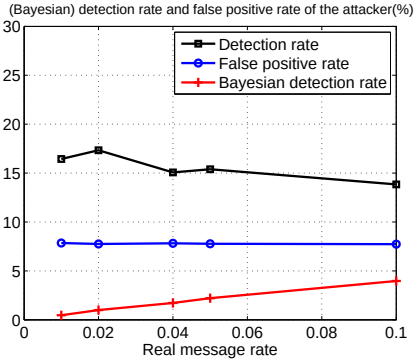

Fig. 8. Gaussian perturbations.

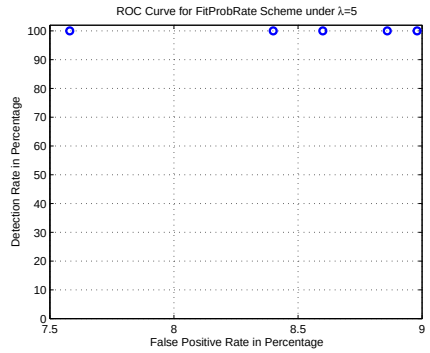

Fig. 9. ROC for FitProbRate scheme.

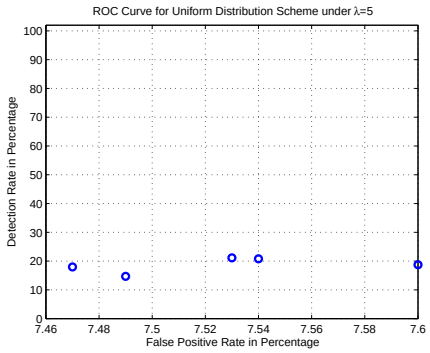

Fig. 10. ROC for Uniform Distribution Scheme.

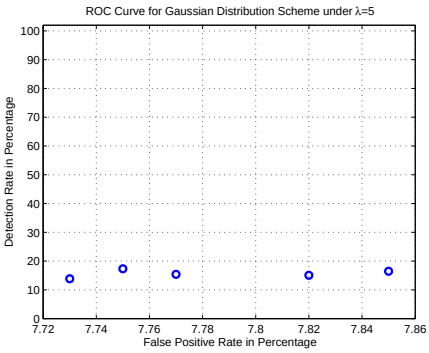

Fig. 11. ROC for Gaussian Distribution Scheme.

Here false positive rate is formulated as following:

Definition 2: Suppose the total number of detected '01' patterns by the attacker is v, the total number of sensors is n, and the number of messages from each sensor is m, then the false positive rate of attacker is defined as:

$$false\ positive\ rate = \frac{v - t}{m \times n - t'}.$$

To better understand the effectiveness of the attacker's detection, we check the Bayesian detection rate [20] of the attacker, which is defined as the probability for an alarm to really indicate a real message. In more detail, we have the following definition:

Definition 3: Suppose the total number of detected '01' patterns by the attacker is v and the number of detected '01' patterns caused by real messages is t, then the Bayesian detection rate of attacker is defined as:

$$Bayesian\ detection\ rate = t/v.$$

Also, to compare the effectiveness of the attacker's detection in different schemes, we draw the Receiver Operating Characteristic (ROC) curve of the attacker, which shows the detection rate as a function of false positive rate.

C. Simulation results

We first use simulation results to validate our security analysis. Then, we compare the performance of two proposed

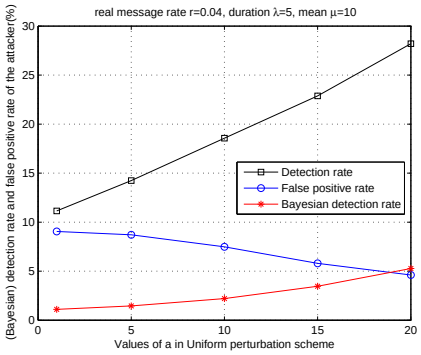

Fig. 12. Impact of a in Uniform perturbation scheme.

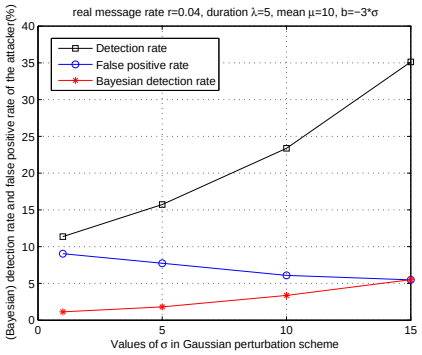

Fig. 13. Impact of σ in Gaussian Perturbation scheme.

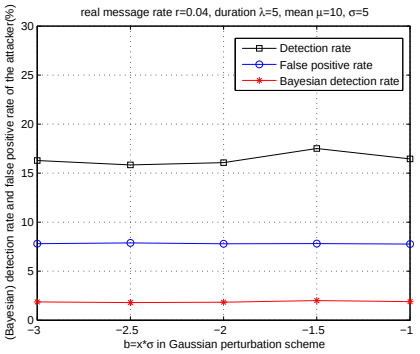

Fig. 14. Impact of b in Gaussian perturbation scheme.

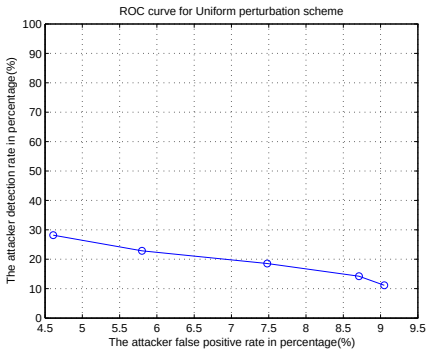

Fig. 15. ROC curve for Uniform perturbation scheme.

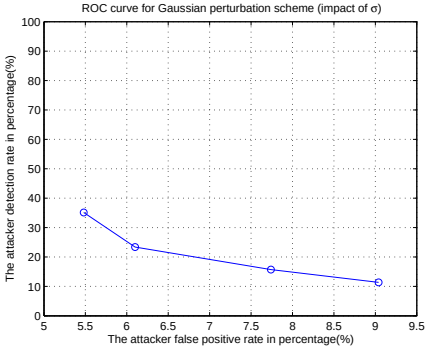

Fig. 16. ROC curve for Gaussian Perturbation scheme (impact of σ).

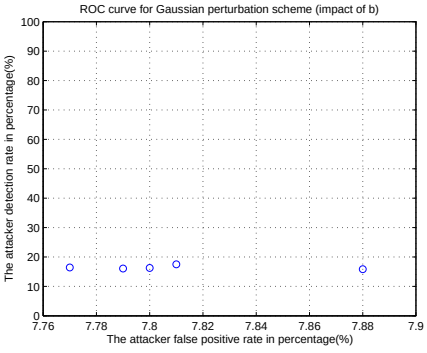

Fig. 17. ROC curve for Gaussian perturbation scheme (impact of b).

schemes and also compare them with the previous schemes, to obtain the insights on which scheme performs better and also show the improvement of our schemes over the previous schemes.

1) Validation of security analysis: First, we run simulations to validate the results of our security analysis. In Figure 3 and Figure 4, we run the simulations in 100 trials to derive the probability of '01' patterns in our proposed schemes. From Figure 3, we can see that the probability of '01' patterns for the Uniform distribution scheme changes around 0.238, which is close to the theoretical result $\frac{1}{4}$. Similarly, the probability of '01' patterns for the Gaussian distribution scheme changes around 0.237, which is close to the theoretical result $\frac{1}{4}$ too, as shown in Figure 4. These match the results of our security analysis well.

Also, from Figure 5, we can see the probability of '01' patterns in percentage changes with the real message rates for the FitProbRate scheme. Again, the simulation results are close to the results of our security analysis, which validate our security analysis.

2) Comparison with previous schemes: Overall, from Figure 6, Figure 7, and Figure 8, we can see that random perturbations following either Uniform distribution or Gaussian distribution can decrease the attacker's detection rate and Bayesian detection rate and increase the attacker's false positive rate significantly.

For example, from Figure 6 to Figure 7, perturbations following Uniform distribution can decrease the attacker's detection rate from around 100% to around 20%. They can also decrease the attacker's Bayesian detection rate from around 20% to less than 5%.

From Figure 6 to Figure 8, we can see that perturbations following Gaussian distribution can further decrease the attacker's performance. For example, the attacker's detection rate is decreased to around 15% and the attacker's Bayesian detection rate is decreased to less than 5%.

From Figure 9, Figure 10, and Figure 11, we can see that the perturbations can make the attacker's detection much less effective, because perturbations lower the attacker's ROC curve significantly. The attacker's detection rate decreases from around 100% to around 20% and around 15% by perturbations following Uniform distribution and Gaussian distribution, respectively.

3) Comparison of two proposed schemes: Comparing from Uniform-distribution scheme to Gaussian-distribution scheme, the attacker's detection rate and Bayesian detection rate are lower from around 20% to around 15% and the false positive rate is slightly higher because the scheme with perturbations following Gaussian distribution has slightly better performance than the Uniform distribution scheme. All of these can be seen from Figure 7 to Figure 8 and from Figure 10 to Figure 11.

4) Impact of different parameters: From Figure 6, we can see that in the FitProbRate scheme if real message rate is higher then the attacker's performance is better: his detection rate and false positive rate almost remain same, but his Bayesian detection rate is higher. Obviously, in this scheme, if real messages appear more frequently with a higher real message rate, this will make the real sources more easily to be detected.

We do not have such observations in our perturbation schemes. From Figure 7 and Figure 8, we can see the impact of real message rate on our perturbation schemes. In both schemes, when real message rate increases, the attacker's false positive rate almost remains the same, but his Bayesian detection rate increases at the cost of a decreasing detection rate. Therefore, the attacker cannot benefit from an increasing real message rate, which shows one advantage of our perturbation schemes.

From Figure 12 and Figure 15, we can see the impact of parameter a in Uniform perturbation scheme. When a increases, the attacker has a better performance: he has a higher detection rate, a higher Bayesian detection rate, and a lower false positive rate. Therefore, when we choose the values for parameter a, it does not mean a larger a is necessarily better.

We notice that if $a = 0$ our scheme becomes a perfect-privacy scheme, because both real and dummy messages follow the same exponential distribution. However, in this scheme, real message latency is high since real message time intervals are not perturbed. Our scheme makes real and dummy message time intervals almost equivalently small. Although it is not as secure as the pure exponential scheme, our scheme trades a certain degree of security for performance. On the other hand, if a is larger, there are larger differences between real and dummy message time intervals, which makes the '01' patterns more obvious. Hence, the attacker has better performance. Also, a larger a means longer running time for our algorithm because it is harder to find positively small time intervals for the real messages, so we should choose an appropriately small value for a (such as $a = 5$).

From Figure 13 and Figure 16, we can see the impact of parameter σ in Gaussian perturbation scheme. It is similar to the impact of a in the Uniform perturbation scheme. When σ is larger, the attacker has a better performance, so when we determine parameter values we should choose an appropriate (small) value (such as 5) for σ, to decrease the attacker's performance.

From Figure 14 and Figure 17, we can see the impact of parameter b in Gaussian perturbation scheme. The attacker's performance does not changes much with the values of b, compared with the other two parameters a and σ.

VII. Related work

In general, privacy preservation in wireless sensor networks could be divided into protecting either sources' or receiver's locations. [21], [22], [23], [16] employ countermeasures against traffic analysis to improve receiver's location privacy, whereas our focus is source location privacy.

To improve source location privacy, [12] proposes phantom routing technique, in which messages are first forwarded by single-path random walk, then they are flooded in the area to reach the base station. Although by employing phantom routing the safety period is significantly improved, when the attacker's hearing range is increased to more than three times larger than that of regular sensors, the attacker's capture likelihood is increased to 97% correspondingly.

[24] and [25] consider a laptop-class eavesdropper in their attack model. [24] proposes four schemes: naive, global, greedy, and probabilistic, to deal with laptop-class attacks. Periodic collection and source simulation are proposed in [25] to protect the context information under a global eavesdropper.

[17] considers node compromise attack and proposes a one-way hash chain based scheme to randomly select intermediate nodes transforming the packets, in order to obfuscate the transmission links from source to destination.

In [15], a global attack model is under consideration. To protect source privacy under such a strong attack model, extra message overhead (i.e., dummy messages) has to be introduced. Otherwise, if all the messages in the network are real messages, then the attacker will know that every message transmission signals a real event. Under this model, the simplest scheme has a constant rate. However, the difficulty in determining this rate reflects a tradeoff among message overhead, real event report latency and privacy. This paper proposes a FitProbRate scheme to reduce real event report latency by relaxing a certain degree of privacy.

Besides these, [9] gives a state-of-the-art survey in privacy preservation techniques for wireless sensor networks. [11] introduces buffering delay to provide temporal privacy, which is suitable for delay-tolerant applications of wireless sensor networks. [26] proposes a cross-layer solution in which the event information is first propagated several hops through a MAC-layer beacon. Then, it is propagated at the routing layer to the destination to avoid further beacon delays. To improve source location privacy, [27] proposes dynamic routing schemes, in which messages are first transmitted to randomly selected intermediate nodes to confuse the attacker.

VIII. Conclusion and Future Work

Recently, source location privacy has become an important research topic for wireless sensor networks. Previous techniques used to protect source location privacy in sensor networks did not solve this topic adequately.

Targeting on solving the problems found in previous schemes, we propose two perturbation schemes that can effectively decrease the attacker's detection capability on real event messages: one based on Uniform distribution and the other based on Gaussian distribution. Our simulation results show that our random perturbation schemes can improve source location privacy significantly compared with previous work, and the scheme based on Gaussian perturbations has better performance than the scheme based on Uniform perturbations.

As future work, we will investigate different attack models and work towards perfect and practical source location privacy solutions.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *CCS*, 2002.

[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Security and Privacy Symposium*, 2003.

[4] W. Du, J. Deng, Y. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *CCS*, 2003.

[5] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *CCS*, 2003.

[6] W. Du, J. Deng, Y.S.Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *IEEE Infocom*, 2004.

[7] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," in *CCS*, 2003.

[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D.Tygar, "Spins: Security protocols for sensor networks," in *Mobicom*, 2001.

[9] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: a state-of-the-art survey," *Ad Hoc Networks*, 2009.

[10] B. Carbunar, Y. Yu, L. Shi., M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," in *SECON*, 2007.

[11] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks," in *ICDCS*, 2007.

[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *ICDCS*, 2005.

[13] Y. Yang, S. Zhu, G. Cao, and T. LaPorta, "An active global attack model for sensor source location privacy: Analysis and countermeasures," in *SecureComm*, 2009.

[14] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in *ACM WiSec*, 2008.

[15] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *IEEE Infocom*, 2008.

[16] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *Infocom*, 2007.

[17] K. Pongaliur and L. Xiao, "Maintaining source privacy under eavesdropping and node compromise attacks," in *Infocom*, 2011.

[18] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "Pda: Privacy-perserving data aggregation in wireless sensor networks," in *Infocom*, 2007.

[19] Y. Yang, M. Shao, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *to appear in ACM Transactions on Sensor Networks*.

[20] S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," in *CCS*, 1999.

[21] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *DSN*, 2004.

[22] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems*, 2006.

[23] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Securecomm*, 2005.

[24] Y. Ouyang, Z. Le, D. Liu, and F. Makedon, "Source location privacy against laptop-class attacks in sensor networks," in *SecureComm*, 2008.

[25] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *ICNP*, 2007.

[26] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. L. Porta, "Cross-layer enhanced source location privacy in sensor networks," in *SECON*, 2009.

[27] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *IEEE Infocom*, 2010.