IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Towards A Statistical Context for Source Obscurity in Sensor Network

[1]Lilavati Samant, [2]Shrikanth N. G.

[1]Computer Science & Engineering Department, VTU University,
SDIT, Mangalore, Karnataka. India

[2] Computer Science & Engineering, VTU University,
SDIT, Mangalore, Karnataka ,India

Abstract - The main aim of the paper is the Source Obscurity in Sensor Network .i.e. Unauthorized Observers must be unable to detect the origin of events by judging the network traffic. This Research presents a new framework for, analyzing and evaluating anonymity in sensor networks .Paper is divided in to two main parts: The first deals with qualitative measure to frame anonymity in wireless sensor network. The second will focus on removal of nuisance parameter by converting it to binary codes. Finally literature indicates how obscurity can be improved using the described framework.

***Keywords* - Wireless Sensor Networks (WSN), source location, privacy, anonymity, nuisance parameters, coding theory.**

1. Introduction

Wireless sensor networks have recently gained much attention in the sense that they can be readily deployed for many different types of missions. In particular, they are useful for the missions that are difficult for humans to carry out.

In many applications, such monitoring networks consist of energy constrained nodes that are expected to operate over an extended period of time, making energy efficient monitoring an important feature for unattended networks. In such scenarios, nodes are designed to transmit information only when a relevant event is detected (i.e., event-triggered transmission). Consequently, given the location of an event triggered node, the location of a real event reported by the node can be approximated within the node's sensing range. There are three parameters that can be associated with an event detected and reported by a sensor node: the description of the event, the time of the event, and the location of the event. When sensor networks are deployed in untrustworthy environments, protecting the privacy of the three parameters that can be attributed to an event-triggered transmission becomes an important security feature in the design of wireless sensor networks .The source anonymity problem in wireless sensor networks is the problem of studying techniques that provide time and location privacy for events reported by sensor nodes.

2. Model Assumption

The first step towards achieving source anonymity for sensor networks in the presence of global adversaries is to refrain from event-triggered transmissions. To do that, nodes are required to transmit fake messages even if there is no data to send. In other words, transmitting real events as soon as they are detected does not provide source anonymity against statistical adversaries analyzing a series of fake and real transmissions.

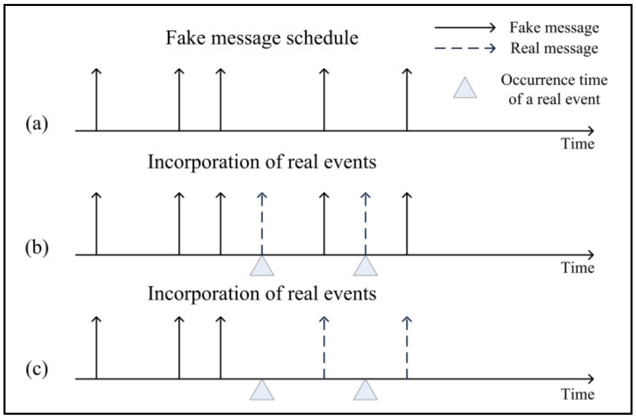

Fake message schedule
Fake message
Real message
Occurrence time of a real event
(a)
Time
Incorporation of real events
(b)
Time
Incorporation of real events
(c)
Time

Fig.1.[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran , 2010, (Fast Abstract).
Different approaches for embedding the report of real events within a series of fake transmissions; (a)shows the pre-specified distribution of fake transmissions,(b) illustrates how real events are transmitted as soon as they are detected, (c) illustrates how nodes report real events instead of the next scheduled fake message.

One way to mitigate the above statistical analysis is illustrated in Figure 1(c). As opposed to transmitting real events as they occur, they can be transmitted instead of the next scheduled fake one. When real events have time-sensitive information, such delays might be unacceptable. Reducing the delay of transmitting real events by adopting a more frequent scheduling algorithm is impractical for most sensor network applications since sensor nodes are battery powered and, in many applications, unchangeable. Therefore, a frequent transmission scheduling will drastically reduce the desired lifetime of the sensor network. The Statistical Source Anonymity (SSA) problem in sensor networks is the study of techniques that prevent global adversaries from exposing source location by performing statistical analysis on nodes transmissions. Practical SSA solutions need to be designed to achieve their objective under two main constraints: minimizing delay and maximizing the lifetime of sensors' batteries.

3. Proposed Framework

3.1 Source Anonymity.

In this section, source anonymity model for wireless sensor networks is being introduced. Intuitively, anonymity should be measured by the amount of information about the occurrence time and location of reported events an adversary can extract by monitoring the sensor network. The challenge, however, is to come up with an appropriate model that captures all possible sources of information leakage and a proper way of quantifying anonymity in different systems.

3.2 Interval in Distinguishability

Currently, statistical anonymity in sensor networks is modeled by the adversary's ability to distinguish between real and fake transmissions by means of statistical analysis. That is, given a series of transmissions of a certain node, the adversary must be unable to distinguish, with significant confidence, which transmission carries real information and which transmission is fake, regardless of the number of transmissions the adversary may observe.

Definition 1 (Interval Indistinguishability) [1]: Let IF denotes a time interval without any real event transmission (called the "fake interval" for the rest of the paper), and IR denotes a time interval with real event transmissions (called the "real interval" for the rest of the paper). The two time intervals are said to be statistically indistinguishable if the distributions of inter-transmission times during these two intervals cannot be distinguished with significant confidence.

3.3 Mapping Statistical Source Anonymity to Binary Hypothesis Testing

In binary hypothesis testing, given two hypothesis, H0 and H1, and a data sample that belongs to one of the two hypotheses (e.g., a bit transmitted through a noisy communication channel), the goal is to decide to which hypothesis the data sample belongs. In the statistical strong anonymity problem under interval indistinguishability, given an interval of intertransmission times, the goal is to decide whether the interval is fake or real (i.e., consists of fake transmissions only or contains real transmissions).That is, given two hypotheses (a real interval and a fake interval) and an observed data (an interval of inter-transmission times of a sensor node), the goal of the adversary is to determine to which hypothesis the observed data belongs (i.e., whether the observed interval contains real event transmissions).

3.4 Nuisance Parameters

In statistical decision theory, the term "nuisance parameters" refers to information that is not needed for hypothesis testing and, further, can preclude a more accurate decision making. When performing hypothesis testing of data with nuisance parameters, it is desired (even necessary in some scenarios) to find an appropriate transformation of the data that removes or minimizes the effect of the nuisance information before performing the hypothesis testing.

4. The Proposed Approach

To improve anonymity, literature suggests introducing the same correlation of inter-transmission times during real intervals to inter-transmission times during fake intervals. That is, let the transmission procedure consists of two different algorithms: AR and AF. In the presence of real events (i.e., in real intervals), algorithm AR is implemented. In the absence of real events (i.e., in fake intervals), algorithm AF is implemented. Algorithm AR is the same as the algorithm. In algorithm AF, the node generates two sets of events independently of each other: "dummy events", dummy events are generated to be handled as if they are real events. That is, dummy events are generated independently of fake messages and, upon their generation, their transmission times are determined according to the algorithm. The purpose of this procedure is to introduce the same correlation of real intervals into fake intervals. That is, not only the two sequences of intertransmission times will be statistically indistinguishable means of statistical goodness of fit tests [11] but also the binary codes representing fake and real intervals will have the same statistical behavior**.** The Anderson-Darlington test is used in both algorithms, AR and AF, to determine the transmission times of real events and dummy events, respectively.

5. Experimental Results

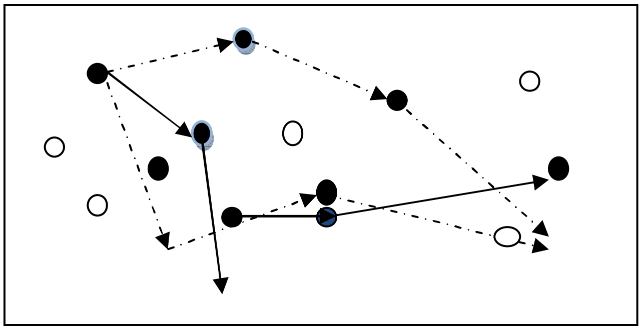
This work is about developing A statistical framework using Java & MySql. Java Simulator is used for simulating Sensor nodes. Since java is platform independent this language is used instead of traditional NS2 simulator. Using AD test in our algorithm AR and AF we have generated fake path by means of random values and real path will remain hidden. File will be encrypted and will be sent in various paths towards destination. Since message will be sent in various paths simultaneously adversaries will get confused. They will try to get the message and if they are on fake path they will fail in getting the message within a limited timeframe and message will reach destination successfully. Then adversary might try the other path thinking that it is real. Once message has been reached it will be useless decrypting it. Even if Adversaries are found to be on Real Path or if adversaries succeed in getting the real path they won’t get the message since the code required decrypting it is with the recipient only and no one else. Message Packet Flow is encrypted in the binary format such that correlations analysis will fail to distinguish between real and fake path. Since the Message is sent at the same time via different paths events are indistinguishable resulting in anonymity of the node from where the message has come.

6. Performance

Proposed Statistical Framework will help to manually delay the message by manually changing the weights assigned to the link connecting Nodes. It can also be used from Any Location and on any platform. Source Obscurity can be demonstrated successfully using this framework.

7. Conclusions

The Source Obscurity can be achieved using the given framework and Binary Hypothesis” concept is being implemented. This Statistical Framework can be improved further for a moving target using more efficient cryptographic techniques.



References

[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, “On Source Anonymity in Wireless Sensor Networks,” in Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks–DSN’10. IEEE Computer Society, 2010, (Fast Abstract)

[2] “Statistical Framework for Source Anonymity in Sensor Networks,” in Proceedings of the 53rd IEEE Global Communications Conference–GLOBECOM’10. IEEE Communications Society, 2010..

[03] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards Statistically Strong Source Anonymity for Sensor Networks,” in Proceedings of the 27th Conference on Computer Communications–INFOCOM’08. IEEE Communications Society, 2008, pp. 466–474..

[04] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy constrained sensor network routing,” in proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks–SASN’04. ACM, 2004, pp. 88–93.

[05] Y. Li and J. Ren, “Source-location privacy through dynamic routing in wireless sensor networks,” in Proceedings of the 29th Conference on Computer Communications – INFOCOM’10. IEEE Communications Society, 2010, pp.1–9.

[06] Y. Xi, L. Schwiebert, and W. Shi, “Preserving source location privacy in monitoring-based wireless sensor networks,” in Proceedings of the 20th IEEE International Parallel & Distributed Processing Symposium–

[07] B. Hoh and M. Gruteser, “Protecting Location Privacy Through Path Confusion,” in Proceedings of the 1st IEEE/ Crenate International Conference on Security and Privacy for Emerging Areas in Communications Networks–SecureComm’05. IEEE Communications Society, 2005, pp.194–205.

[08] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, “Towards event source unobservability with minimum network traffic in sensor networks,” in Proceedings of the first ACM conference on Wireless network security–WiSec’08. ACM, 2008, pp. 77–88.

[09] N. Li, N. Zhang, S. Das, and B. Thuraisingham, “Privacy preservation in wireless sensor networks: A state-of-the-art survey,” Elsevier Journal on Ad Hoc Networks, vol. 7, no. 8, pp. 1501–1514, 2009.

[10] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks–SECON'09. IEEE Communications Society, 2009, pp. 493–501.

[11] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984

[12] M. Stephens, "EDF statistics for goodness of fit and some comparisons," Journal of the American Statistical Association, vol. 69, no. 347, pp. 730–737, 1974. Science,1989.

Lilavati Samant. Is a M.Tech Student of Computer Science & Engineering Department of SDIT, Mangalore. She graduated with BE (Honours') in Information Technology from Goa University, Goa. She is currently pursuing her Masters in Computer Science & engineering at SDIT (Shree Devi College of Engineering).Her research Areas are Computer Networks, Wireless Sensor Networks and Cryptography**.**

Mr.Shrikant is an Assistant Professor in the Department of Computer Science & Engineering, affiliated to VTU university, at SDIT(Shree Devi College of Engineering).His research areas are: Computer Network, Database