International Journal of Science Engineering and Advance Technology

A Security Measure That Quantify The Anonymity Of Different Systems

[1]Satyasudheer Yalla, [2]M.VamsiKrishna
1,2Dept, Of CSE.Chaitanya Institute of Science & Technology,Kakinada,AP,India

Abstract:

The basis ambiguity difficulty in wireless sensor networks is the trouble of studying methods that provide time and position privacy for events reported by sensor nodes. Time and location privacy will be used interchangeably with source anonymity throughout the paper. The source anonymity problem has been drawing growing research concentration recently the source anonymity problem has been addressed under two different types of adversary's namely local and global adversaries. A local adversary is definite to be an adversary having limited mobility and inequitable view of the network traffic. Routing based methods have been shown to be efficient in hiding the locations of reported events against local adversaries. A global adversary is defined to be an adversary with capacity to check the traffic of the entire network e.g. coordinating adversaries spatially distributed over the network. Against global adversaries routing based techniques are known to be unproductive in cover up location information in event-triggered transmission.

Keywords: Wireless sensor networks (WSN), source location, privacy, anonymity, hypothesis testing, nuisance parameters, coding theory.

Introduction:

There is an understood supposition of the use of a probabilistic distribution to plan the transmission of fake messages. On the other hand the arrival distribution of real events is in general time-variant and unknown a priori. If nodes report real events as soon as they are detected independently of the distribution of fake transmissions given the acquaintance of the fake transmission distribution statistical analysis can be used to recognize outliers real transmissions with a possibility higher than 1/2. In other words transmitting real events as soon as they are noticed does not provide source anonymity against statistical adversaries analyzing a series of fake and real transmissions. The first step toward realizing source anonymity for sensor networks in the company of global adversaries is to abstain from event-triggered transmissions. To do that nodes are necessary to transmit fake messages even if there is no discovery of events of interest real events will be used to indicate events of interest for the rest of the paper. When a real event occurs its report can be entrenched within the transmissions of fake messages. Consequently given an individual transmission an observer cannot conclude whether it is fake or real with a possibility considerably higher than 1/2 presumptuous messages are encrypted. For example believe programming sensor nodes to deterministically transmit a fake message every minute. If a real event occurs within a minute from the last transmission its report must be postponed until exactly 1 minute has elapsed. This approach though introduces additional delay before a real event is reported.

Related Work:

Communication is supposed to take place in a network of energy inhibited sensor nodes. Nodes are organized to sense events of interest and statement them with minimum delay. As a result given the location of a certain node the position of the reported event of interest can be approximated within the node's communication variety at the time of transmission. When a node senses an event it places information about the event in a message and transmit an encrypted version of the message. To difficult to understand the report of an event of interest nodes are supposed to broadcast fake messages even if no event of interest has been detected. Nodes are also assumed to be able to with a semantically secure encryption algorithm so that opponents are not capable to differentiate between the reports of events of interest and the fake transmissions by means of cryptographic tests. In addition the network is supposed to be deployed in an out-of-the-way environment and therefore the preservation of nodes' energy is a intend prerequisite.

Existing Method:

A local adversary is defined to be an adversary having limited mobility and partial view of the network traffic. Routing based techniques have been shown to be effective in hiding the locations of reported events against local adversaries. A global adversary is defined to be an adversary with ability to monitor the traffic of the entire network. Against global adversaries routing based techniques are known to be unproductive in hiding location information in event-triggered transmission. Encrypting a message before transmission for example can hide the context of the message from unauthorized observers but the mere existence of the cipher text is indicative of

information transmission. In the existing literature the source vagueness problem has been addressed under two different types of adversaries' namely local and global adversaries. This is due to the fact that since a global adversary has full spatial view of the network it can immediately detect the origin and time of the event-triggered transmission. While transmitting the description of an intelligence event in a private manner can be achieved via encryption primitives hiding the timing and spatial information of reported events cannot be achieved via cryptographic means.

Disadvantages:

The source anonymity problem has been drawing increasing research concentration recently. The source anonymity problem in wireless sensor networks is the trouble of studying techniques that provide time and location privacy for events reported by sensor nodes. Time and location privacy will be used interchangeably with source anonymity all through the paper.

Proposed Method:

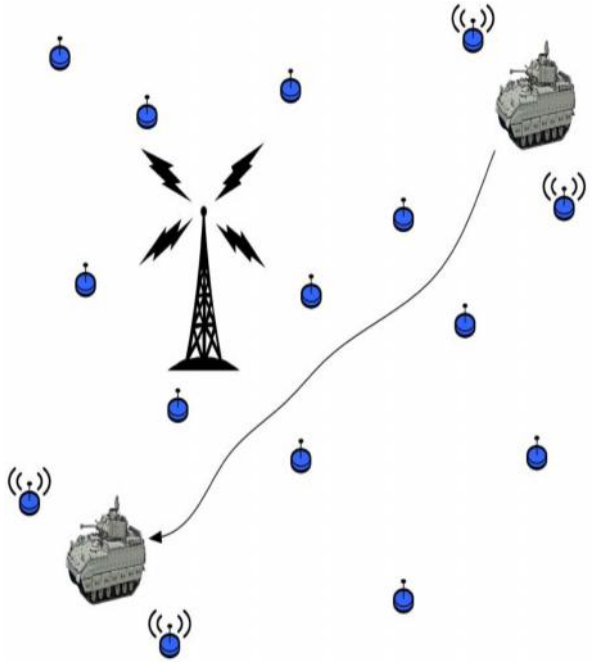
In particular realizing that the SSA problem can be mapped to the hypothesis testing with nuisance parameters involves that breaching source anonymity can be transformed to finding an suitable data transformation that removes the nuisance information. By finding a transformation of observed data we change the problem from analyzing real-valued examples to binary codes and recognizes a possible anonymity breach in the current solutions for the SSA problem. We examine the difficulty of statistical source anonymity in wireless sensor networks. We bring in the notion of interval in-distinguishability and demonstrate how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability. We propose a quantitative measure to estimate statistical source anonymity in sensor networks. We map the problem of violating source anonymity to the statistical trouble of binary hypothesis testing with nuisance parameters. We exhibit the significance of mapping the problem in hand to a well-studied problem in uncovering hidden vulnerabilities.

Advantages:

Removes or minimize the effect of the nuisance information.

Sensor Network Architecture:

By finding a transformation of observed data we change the problem from analyzing real-valued examples to binary codes and recognizes a possible anonymity breach in the current solutions for the SSA problem. In particular realizing that the SSA problem can be mapped to the hypothesis testing with nuisance parameters involves that breaching source anonymity can be transformed to finding an suitable data transformation that removes the nuisance information.



Source Anonymity:

We propose a quantitative measure to calculate statistical source anonymity in sensor networks. We initiate the concept of interval indistinguishability and demonstrate how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability.

Coding Theory:

By finding a alteration of observed data we adapt the problem from analyzing real-valued samples to binary codes and make out a possible anonymity breach in the current solutions for the SSA problem. We analyze existing solutions under the proposed model.

Nuisance Parameters:

When performing hypothesis testing of data with nuisance parameters it is needed even necessary in some scenarios to find a suitable transformation of the data that take away or diminish the effect of the nuisance information. In statistical decision theory the term nuisance parameters refers to information that is not essential for hypothesis testing and additionally can rule out a more precise decision making.

Hypothesis Testing:

In the statistical strong anonymity problem under interval in distinguishability given an interval of intertransmission times the goal is to decide whether the interval is false or real i.e. consists of fake transmissions only or contains real transmissions. In binary hypothesis testing given two hypothesis H0 and H1 and a data trial that fit in to one of the two hypotheses e.g. a bit transmitted through a noisy communication channel and the objective is to make a decision to which hypothesis the data sample belongs.

ALGORITHM USED:

INPUT: location information L and time information T

OUTPUT: accept the hypothesis H_0 or H_1

curr_loc=L

curr_time=T

if n>0 then

compute $T_0(n)$ and $T_1(n)$

compute speed 0 from curr_loc and prev_loc, curr_time and prev_time

if 0>V_{max} then

w_n=w_n+1

end if

if w_n>=$T_1(n)$ then

Accepts the hypothesis h_1 and terminate the test

end if

if w_n<=$T_0(n)$ then

initialize n and w_n to 0 and accepts the hypothesis H_0

return;

end if

end if

n=n+1

prev_loc=curr_loc

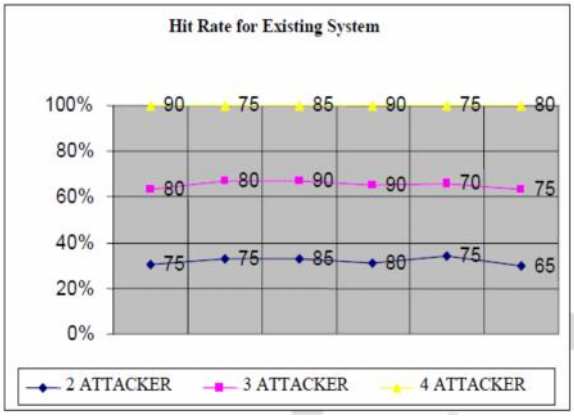
prev_time=curr_time

HIT RATE:

$$\min_{\mathbf{w},b,\xi} \ \frac{1}{2}\mathbf{w}^T\mathbf{w} + C\sum_{i=1}^{l}\xi_i$$
$$\text{Subject to} \ \ y_i(\mathbf{w}^T\phi(x_i)+b) \geq 1-\xi_i,$$
$$\xi_i \geq 0.$$

Its dual is

$$\min_{\alpha} \ \frac{1}{2}\alpha^T Q\alpha - \mathbf{e}^T\alpha$$
$$\text{Subject to} \ \ \mathbf{y}^T\alpha = 0,$$
$$0 \leq \alpha_i \leq C, \quad i = 1,\ldots,l,$$



CONCLUSION:

We give a statistical framework based on binary hypothesis testing for modelling, analyzing and calculating statistical source anonymity in wireless sensor networks. We bring in the idea of interval indistinguishability to model source location privacy. We showed that the current advances for scheming statistically anonymous systems bring in association in real intervals while false intervals are uncorrelated. By mapping the difficulty of detecting source information to the arithmetical problem of binary hypothesis testing with nuisance parameters we showed why previous studies were not capable to notice the source of information break out that was established in this paper. After all we proposed an alteration to existing solutions to get better their ambiguity against correlation tests. Future conservatory to this work include mapping the difficulty of statistical source anonymity to coding theory in order to map an knowledgeable system that encourage the concept of interval indistinguishability.

REFERENCES:

[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "On Source Anonymity in Wireless Sensor Networks," Proc. IEEE/IFIP 40th Int'l Conf. Dependable Systems and Networks (DSN '10), 2010.

[2] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical Framework for Source Anonymity in Sensor Networks," Proc. IEEE GlobeCom, 2010.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[4] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," Proc. IEEE 13th

Mediterranean Conf. Control and Automation (MED '05), pp. 719-724, 2006.
[5] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless Sensor Network Survey," Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008.
[6] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), pp. 41-47, 2002.
[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.
[8] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," Proc. Eighth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '06), pp. 46-59, 2006.
[9] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra- Lightweight Block Cipher," Proc. Ninth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '07), pp. 450-466, 2007.
[10] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE 15th Int'l Conf. Network Protocols (ICNP '07), pp. 314-323, 2007.
[11] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, pp. 466-474, 2008.
[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS '05), pp. 599- 608, 2005.
[13] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 88- 93, 2004.
[14] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, and U. Lowell, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. IEEE Seventh Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WOWMOM '06), pp. 32-41, 2006.
[15] X. Wang, X. Li, Z. Wan, and M. Gu, "CLEAR: A Confidential and Lifetime-Aware Routing Protocol for Wireless Sensor Network," Proc. IEEE 20th Ann. Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC '09), pp. 2265-2269, 2009.
[16] Y. Li and J. Ren, "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1-9, 2010.
[17] Y. Xi, L. Schwiebert, and W. Shi, "Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks," Proc. IEEE 20th Int'l Parallel & Distributed Processing Symp. (IPDPS '06), pp. 1-8, 2006.
[18] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," Proc. IEEE/CreatNet First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), pp. 194-205, 2005.
[19] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. First ACM Conf. Wireless Network Security (WiSec '08), pp. 77-88, 2008.
[20] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey," Elsevier J. Ad Hoc Networks, vol. 7, no. 8, pp. 1501-1514, 2009.

Mr SatyaSudheer Yalla is a student of Chaitanya Institute Science of Technology, MadhavaPatnam, Kakinada,Under JNTU Kakinada. He received his B.Tech in Computer Science & Engineering from Kims Engineering college, Amalapuram. Under AndraUniversity, Vishakapatanam. Presently he is pursuing his M.Tech (Computer Science & Engineering) from this college. His area of interest includes Computer Networks, Network Securities, ERP Systems and Object oriented Programming languages, all current trends and techniques in Computer Science.

Sri.**M.Vamsi krishna**, well known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra University is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications..