Asian Journal of Computer Science and Technology (AJCST)
Vol.2 .No.1 2014 pp 43-48
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

APPLICATION OF CODING THEORY TO SOURCE ANONYMITY IN WIRELESS SENSOR NETWORKS

Swathika.M, Mrs. Kavitha.T
swathika.murugan@gmail.com

ABSTRACT

The locations of events in applications like military reported by a sensor network need to remain anonymous. This problem has emerged as an important topic in the security of wireless sensor networks.An unauthorised observer detects the origin of events by analysing the network traffic. 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. The binary codes in coding theory are used to send the real event along with the fake message using the interval in-indistinguishability and thus the anonymity is maintained.

Index Terms-adversary, anonymity, coding theory, privacy, security, wireless sensor networks

1. INTRODUCTION

A sensor network has multiple detection stations which is known as sensor nodes, which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. [1] The power for each sensor node is derived from the electric utility or from a battery.

Wireless sensor network is a spatially distributed autonomous sensor to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; [4][5]

Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Event detection is used to detect the current event that happened in the location that is to be sensored. 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.[2]

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.

The source anonymity problem has been addressed under two different types of adversaries, namely, local and global adversaries. [1]

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. [12][13]

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.

Coding theory is the study of the properties of codes and their fitness for a specific application. Codes are used for data compression, cryptography, error-correction and more recently also for network coding.

Data compression is used to reduce the network load and make files smaller. The second, channel encoding, adds extra data bits to make the transmission of data more robust to disturbances present on the transmission channel. The ordinary user may not be aware of many applications using channel coding.

2. RELATED WORKS

One of the strategies, a technique called phantom routing, has proven flexible and capable of protecting the source's location, while not incurring a noticeable increase in energy overhead. Further, examined the effect of source mobility on location privacy. Even with the natural privacy amplification resulting from source mobility phantom routing techniques yield improved source-location privacy relative to other routing methods.Introducing the technique called phantom routing, has proven flexible and capable of protecting the source's location, while not incurring a noticeable increase in energy overhead.

Achieving source location privacy using phantom routing provides significant privacy amplification. Location-privacy techniques built using network security mechanisms, [16] such as the anonymity provided by mixes, incur additional communication, memory and computational overhead that are prohibitive for use in resource-constrained environments.[2]

Sensing the tasks, potential sensor networks applications are explored. The flexibility, fault tolerance high sensing fidelity and low-cost characteristics of sensor networks create many new and exciting application areas for remote sensing. However realization of sensor networks needs to satisfy the constraints by factors such as fault tolerance, scalability etc., and these constraints are highly stringent and specific, new wireless ad hoc networking techniques are needed. [4]

Wireless sensors and wireless sensor networks have come to the forefront of the scientific community recently. This is the consequence of engineering increasingly smaller sized devices, which enable many applications. The use of these sensors and the possibility of organizing them into networks have revealed many research issues and have highlighted new ways to cope with certain problems. In this paper, different applications areas where the use of such sensor networks has been proposed are surveyed. In this paper, different application areas where the use of such sensor networks has been proposed are surveyed. The possible use of wireless sensor motes and networks extends over a vast area of human activity. Still most are under research there is a remarkable effort and progress. Adding the parameter "mobility" creates another dimension to the information system. [5]

Localization is a way to determine the location of sensor nodes. Localization of sensor nodes is an interesting research area, and many works have been done so far. It is highly desirable to design low-cost, scalable, and efficient localization mechanisms for WSNs. In this paper, we discuss sensor node architecture and its applications, different localization techniques, and few possible future research directions. The goal of the survey is to present a comprehensive review the literature of various aspects. Wireless sensor networks are designed for specific application. Application like environmental monitoring, military target tracking etc., Still many issues to be resolved around WSN applications such as communication architectures, security and management.[6]

When source location privacy is of critical importance, special attention must be paid to the design of the node transmission algorithm so that monitoring sensor nodes does not reveal private source information. One of the major challenges for the source anonymity problem is that it cannot be solved using traditional cryptographic primitives. Encrypting nodes' transmissions, for instance, can hide the contents of plaintext messages, but the mere existence of cipher texts is indicative of information transmission. Preserving source location privacy is the method used here. It provides source anonymity but still there are some leakages. Development of a stronger statistical framework that can properly model source anonymity in wireless sensor networks.[7]

Analysing existing solutions for designing anonymous sensor networks using the proposed model.Showing how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information.

By doing so, it transforms the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be

incorporated into the study of anonymous sensor networks.

If nodes report real events as soon as they are detected, given the knowledge of the fake transmission distribution, statistical analysis can be used to identify real transmissions. When real events have time sensitive information, such delays might be unacceptable.

The wireless sensor networks are a network where there is lack of security. And so, security is to be provided via anonymity in a network. So, the intuition is that to provide anonymity in a network where the information sent should be secure or not known to the unauthorised users.

3. MODEL ASSUMPTIONS

A. Network Model

Communication is assumed to take place in a network of energy constrained sensor nodes. Nodes are deployed to sense events of interest and report them with minimum delay. Consequently, given the location of ascertain node, the location of the reported event of interest can be approximated within the node's communication range at the time of transmission. When a node senses an event, it places information about the event in a message and broadcast an encrypted version of the message.[6][7][8][9] To obscure the report of an event of interest, nodes are assumed to broadcast fake messages, even if no event of interest has been detected. Nodes are also assumed to be equipped with a random distribution method, so that adversaries are unable to distinguish between the reports of events of interest(real event) and the fake transmissions by means of cryptographic tests. Furthermore, the network is assumed to be deployed in an unreachable environment and, therefore, the conservation of nodes' energy is a design requirement.

B. Adversarial Model

The adversarial models can be of external, passive, and global [2][3][4].

An external adversary is an adversary who does not control any of the nodes in the network. As opposed to active adversaries injecting their own traffic or jamming the network, a passive adversary is only capable of observing the network traffic.

A global adversary is an adversary who can monitor the traffic of the entire network and can determine the node responsible for the initial transmission reporting an event of interest.

The justification behind this model is twofold. First, it serves as a worst case scenario, when the coverage area of the adversary is time varying and/or unknown.

Second, it represents a network of collaborating adversaries that can cover the deployed sensor network. The adversary is also assumed to know the distribution of fake message transmissions. Furthermore, the adversary is assumed capable of observing nodes transmissions over extended periods of times and performing sophisticated statistical analysis to compare the observed transmission with the known distribution of fake messages.[11] The adversary, however, is not assumed able to break the security of the encryption algorithm and distinguish the report of event of interests via cryptographic tests.

C. Interval Indistinguishability

Let IF denotes a time interval without any real event transmission called the fake interval and I_R denotes a time interval with real event transmission called the real interval. 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. [1][7][8]

Given the notion of interval in-distinguishability, consider the following game between a challenger, C (the system designer), and a statistical adversary, A.

D. Anonymity game

1. C chooses two intervals IR and IF, in which IR is a real interval and IF is a fake one.
2. C draws a bit b € {0,1} uniformly at random and sets

IR = Ib and IF = Ib´, where b denotes the binary complement of b.

3. C gives Ib and Ib´ to A.
4. A makes any statistical test of her choice on Ib and Ib´ and outputs a bit b´.
5. If b´=b, A wins the game.

Game 1 can be viewed as a standard binary hypothesis testing problem. 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 belong (i.e., whether the observed interval contains real event transmissions).

Inter-transmission times during fake intervals are iid's, while inter-transmission times during real intervals are neither independent nor identically distributed. In theory, the only way to guarantee that a

sequence of random variables is statistically indistinguishable from a given iid sequence is to generate it as an iid sequence with the same distribution. The notion of interval in-distinguishability, suggests a different approach for the design of anonymous sensor networks.

Interval in-distinguishability does not impose any requirements, such as iid, on the distribution of inter-transmission times during fake intervals. Therefore, designing fake intervals with the distribution that is easiest to emulate during real intervals is the most logical solution. This idea opens the door for more solutions as it gives more flexibility for system designers. [12] To improve anonymity, we suggest introducing the same correlation of inter-transmission times during real intervals to inter-transmission times during fake intervals.

E. Random distribution

The method used is random distribution method which is discrete in nature. A random variable assigns a number of values to some outcome. This plays in two conditions:

If the possible values are at distinct points, then the random variable is said to be DISCRETE.

If the possible values are an interval of values, then the random variable is said to be CONTINUOUS.

Discrete Random Variable – usually it is a count data e.g.: [Number of]

- one that takes on a countable number of values which means listing all possible outcomes without missing any values, although it might take an infinite amount of time.

X = values on the roll of two dice:

X has to be either 2, 3, 4… or 12.

Y = number of accidents on the UTA campus during a week:

Y has to be 0, 1, 2, 3, 4, 5, 6, 7, 8, …… "real big number"

Examples for the random variable are: Dead/alive, treatment/placebo, dice, counts, etc.

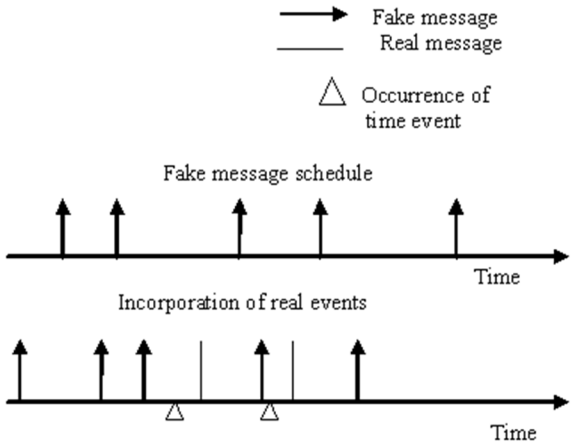
Let Xi be the random variable representing the time between the ith and the i+1st transmissions and let the desired mean of these random variables be μ; i.e., IE[Xi]=μ, for all i (since the Xi's are iid).

F. Fake Interval (IF)

In the absence of real events, nodes are programmed to transmit iid fake messages according to a pre-specified probability distribution. That is, the X_is in fake intervals are iid random variables with mean μ.Therefore , during any fake interval,I_F,for any X_{i-1} , X_i € I_F, one gets

$$IE[X_i \mid X_{i-1} < \mu] = \mu,$$

By the fact that X_{i-1} and X_i are independently by definition and that IE [X] = μ, for all j's



This shows an illustration of solutions based on statistical goodness of fit tests. Nodes transmit fake messages according to a pre-specified probabilistic distribution and maintain a sliding window of inter-transmission times. When a real event occurs, it is transmitted as soon as possible under the condition that the samples in the sliding window maintain the designed distribution. The transmission following the real transmission is delayed to maintain the mean of the distribution of inter-transmission times in the sliding window.

G. Real Interval (IR)

By definition, real intervals will have both fake and real transmissions. Let E_i be the random variable representing the type of the event reported in the ith transmission, i.e., fake or real. Then, E_i can take the values R and F, where R denotes a real event and F denotes a fake one. Since, in the most general scenario, the distribution of inter-arrival times of real events can be time variant and unknown beforehand, we will assume that E_i can take the values R and F with arbitrary probabilities. Recall that the time between the transmission of a real event and its preceding fake one is usually shorter than the mean μ by design (to reduce delay).

Recall further that the time between the transmission of a real event and its successive one is usually longer than μ by design (to adjust the ensemble

mean). That is, during any real interval, I_R, for any X_{i-1}, X_i € I_R, one gets

$$IE[X_i \mid X_{i-1} < \mu, E_i = R] > \mu, \quad (1)$$

and

$$IE[X_i \mid X_{i-1} < \mu, E_i = F] > \mu, \quad (2)$$

Combining (1) and (2), we get

$$IE[X_i \mid X_{i-1} < \mu] = IE[X_i \mid X_{i-1} < \mu, E_i = R].Pr[E_i = R] + IE[X_i \mid X_{i-1} < \mu, E_i = F].Pr[E_i = F]$$

$$> \mu.Pr[E_i = R] + \mu.Pr[E_i = F] = \mu.$$

An inter-transmission time can be either shorter or longer than μ.The inter-transmission time that is shorter than μ is "short inter-transmission time" and an inter-transmission time that is longer than is μ "long inter-transmission time." The short inter-transmission times are most likely to be followed by long inter-transmission times[14] during real intervals. The short inter-transmission times followed by long inter-transmission times occur more frequently in real intervals than fake intervals. A short-long pattern will be used to denote a short inter-transmission time followed by a long inter-transmission time). This shows the short- long patterns.

3. PROPOSED SYSTEM

The proposed work is to provide anonymity to the source in the network.

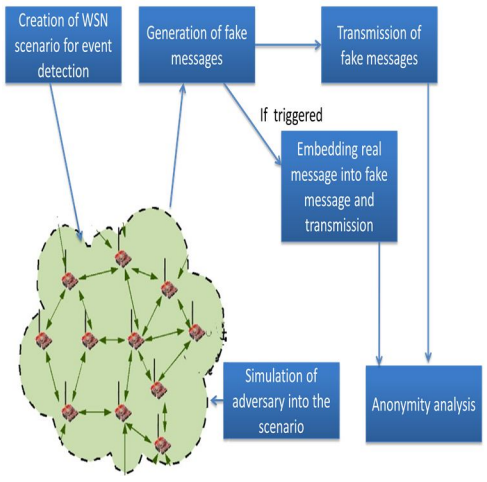


Figure.1. Architecture Diagram

The wireless sensor networks scenario is created for the event detection. Fig 1.shows the architecture diagram where the system computation is realized through the application of four main modules implemented in ns2. Event detection has three parameters reported by a sensor node: the description of the event, the time of the event, and the location of the event. The modules can be generation of fake messages where the message is generated using the random distribution, transmission of fake messages when the real message is not detected, embedding real message into fake message when triggered or detected and then the anonymity can be analysed.

4. IMPLEMENTATION AND RESULTS

The nodes are created and the fake messages are generated for the purpose of providing the anonymity.The tool used is NS2. It is a discrete event simulator for networking research.

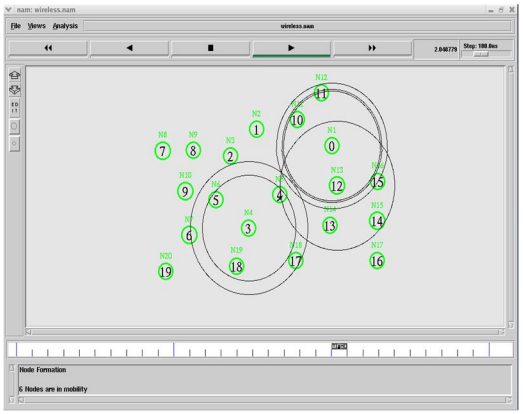


Figure 2. Orientation

The message can be passed within that orientation, the action of orienting someone or something relative to the points of a compass or other specified positions. So that the node formation is done and there are six nodes which is in mobility.

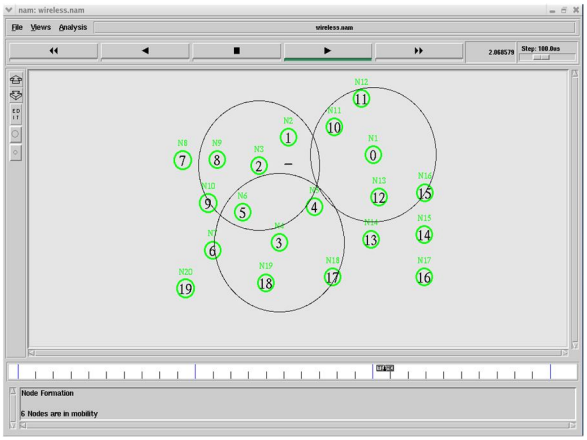


Figure.3. Message passing

This figure deals with the message that is (fake message) passed from node 0 to node 2.The node 2 will send message to node 5 which is the destination node. Message passing in computer science is a form of communication used in concurrent computing, parallel computing, object-oriented programming, and inter-process communication. In this model, processes or objects can send and receive messages (comprising zero or more bytes, complex data structures, or even segments of code) to other processes. By waiting for messages, processes can also synchronize.

5. CONCLUSION

The proposed system satisfies the statistical source anonymity using the random distribution method. The notion of interval in-distinguishability is introduced to model the source location privacy. By converting the problem from analyzing real-valued samples to binary codes using coding theory which is identified a possible anonymity breach. The fake message is generated and real message is sent along with the fake one using ns2 simulation. Here the orientation and the message is also passed. Future work will satisfy the application of coding theory where the anonymity will be analysed and designed.

REFERENCE

[1] M.Shoa,Y.Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, pp. 466-474, 2008.

[2] 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.

[3] 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.

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

[5] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Net- works," Proc. IEEE 13th Mediterranean Conf. Control and Automation (MED '05), pp. 719-724, 2006.

[6] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless Sensor Network Survey," Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008

[7] 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.

[8]Yi Ouyang , Zhengyi Le, and YurongXu, "Providing Anonymity in wireless sensor networks", pp. 812-922, 2013.

[9] Philip Reindel, Xiao jiang Du , Kendall Nygard and Hongli Zhang , "Lightweight Source Anonymity in Wireless Sensor Networks" pp, 93-119, 2011.

[10] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen,"A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks" Proc. IEEE INFOCOM, 2012.

[11] Osianoh Glenn Aliu, Student Member, IEEE, Ali Imran, Member, IEEE, Muhammad Ali Imran Member, IEEE, and Barry Evans, Senior Member, IEEE, "A Survey of Self Organisation in Future Cellular Networks" Proc. IEEE INFOCOM,2013.

[12] Tao Chen, Member, IEEE, Zheng Yang, Member, IEEE, Yunhao Liu, Senior Member, IEEE, Deke Guo, Member, IEEE, and Xueshan Luo, "Localization-Oriented Network Adjustment in Wireless Ad Hoc and Sensor Networks" Proc. IEEE INFOCOM,2014.

[13] T.kavitha and D.Sridharan,"Security of vulnerabilities in wireless sensor networks:A Survey", Journal of Information Assurance and security 5 (2010) 031-044.

[14]Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in WiSec '08: Proceedings of the first ACM conference on Wireless network security. New York, NY, USA: ACM, 2008, pp.77–88.

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

[16]T.kavitha and D.Sridharan, "Probabilistic key chain based key distribution schemes for Wireless sensor networks", International review on computers and software, Praise Worthy Prize, Italy, May 2013, (vol 8 No.5) pp. 1156-1169.