Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.260 – 264

RESEARCH ARTICLE

An Approach for Efficient Way to Evaluate Statistical Source Anonymity in Wireless Sensor Network

Harshal S. Bhagwat[1], Poonam P. Borkar[2]

[1]Computer Science & Engineering Department & S.G.B.A. University, India

[2]Computer Science & Engineering Department & S.G.B.A. University, India

[1] harshalbhagwat123@gmail.com; [2] poonam.borkar@raisoni.net

Abstract*— *In some critical applications, the locations of events reported by a sensor network need to remain anonymous. Means that, when unauthorized observer monitor or analyse the network traffic, observer must be unable to seem the origin of such events which will be transmitted. And this is said to the source anonymity problem; this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this, present a new structure for modeling means that to model for the network, analysing means to analyze the network, and evaluating anonymity in sensor networks. The novelty of the proposed framework is two steps: first, it will introduces the idea of "interval indistinguishability" and provides a quantitative measure to model anonymity in wireless sensor networks; and second, it will maps source anonymity to the statistical problem of binary hypothesis testing with some parameters. This works target to the Statistical Source Anonymity (SSA) 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 objectives: minimizing delay and maximizing the lifetime of sensors batteries and also the security approach.

Keywords*— *Adversary, Statistical Source anonymity, Indistinguishability, Nuisance parameters

I. INTRODUCTION

In networks there are different kinds of networks are available and some of them are wireless, and many more. In Wireless Sensor networks, mostly sensor networks are employed to sense, monitor means watch on network traffic, and report events of interest in a several range of applications including, but there is no limited to, military means in battlefield, health care means patients in hospitals, and animal tracking means we taken an example of panda in forest. In different applications scenario, such monitoring the traffic networks consist of sensor nodes which will be operated and running on the energy constrained, that are needs to be operate over a long period of time, and making low energy consumed monitoring an important aspect for unattended the traffic

networks. In these fashions, when a related sensed event is detected at source node then it will transmits the information (event-triggered transmission). Because, given the location of an event-triggered transmission from node, the source location of a sensed events reported by the node can be within the node's sensing range in network.

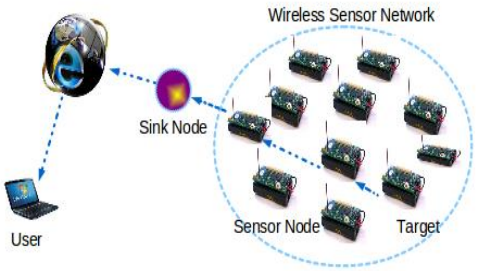

Figure 1: Data send from node to user in network

Adversary observing nodes transmissions of events so the locations of the node at different time intervals can be revealed, after analysing the network traffic. There are three parameters that are associated with a sensed event detected and reported by a sensor node, first is the description of the event, second is the time of the event, and the last one is location of the event. At the first time when sensor networks is to be employed in untrustworthy environments, protecting the above mentioned three parameters that can be related to an event triggered transmission makes an important security feature in designing of wireless sensor networks. When the "description" of a sensed event at source node in a private manner can be transmitted and get via encryption primitives, anonymous of the timing and spatial information of sensed and reported events cannot be gain via cryptographic terms. Encrypting a sensed event before transmission, for instance, can hide the original message from unauthorized observers or form adversaries, but just the existence of the cipher text or called as unreadable text is indicate that of information transmission. Therefore this source anonymity problem in wireless sensor networks is the problem of studying the techniques which will provides location privacy and time for events reported by sensed nodes.

II. LITERATURE SURVEY

Wei Tan et al [1], Source location privacy protection is a significant security property of sensor networks used to collect information about monitored objects in military or endangered species monitoring applications. Secure routing protocols should be designed to prevent adversaries from finding out the source through hop-by-hop backtracking. To this aim, PEM is proposed to provide strong protection for source location privacy where fake sources are generated dynamically and several fake paths are formed and extended in the network. Adversaries would be induced farther away from the source if they are entrapped by some of the fake paths. It performs quite well even though an object occurs near the base station. The theoretical and simulation results show that PEM can provide strong source-location privacy protection with minimal message latency and acceptable overhead.

Mauro Conti et al [2], provided a survey of the literature in source location privacy (SLP) for wireless sensor networks(WSNs). Then, discussed some of the works that have a high influence on the state of the art today, together with the concepts that they introduced. These concepts included anonymity, unobservability, safety period, capture likelihood, unsink ability, contextual privacy, identity privacy, location privacy, timing privacy, and route privacy. Next, included a classification of the adversary based on its behavior, view of the network, and the information exposed by the network to the adversary.

B. Alomair etal [3] provided a statistical scenario which will be depend on binary hypothesis testing for modeling, analyzing, and evaluating statistical source anonymity in wireless sensor networks. In this also introduced the notion of interval indistinguishability to model source location privacy. In this the current scenario for designing statistically anonymous systems introduces correlation in real intervals and fake intervals are uncorrelated. By mapping the problem of detecting sensed source information to the statistical problem of binary hypothesis testing with some parameters.

Yun Li et al [4], proposes and states that, SLP is critical to the successful employment of Wireless Sensor Networks for many applications. The proposed criteria is for quantitatively measure Source Location Privacy for routing-based schemes. Depend on this criteria, the proposed a scheme that can achieve Source Location Privacy in Wireless Sensor Networks through a two-steps routing, i.e. one is routing to a single RSIN and routing through the NMR. The optimal location for the mixing ring is also derived. The above approach provides provable local Source Location Privacy and global Source Location Privacy. And the simulation results showed that while assuring a high message delivery ratio the proposed scheme can give good performance in energy consumption and message delivery latency.

Parv Venkitasubramaniam et al [5], proposed the main contributions of an analytical approach to anonymous wireless networking. To the best of our knowledge, the proposed metric is the first analytical measure designed to quantify the secrecy of routes in an eavesdropped wireless network. The preliminary results obtained so far clearly demonstrate the potential for analytical methods to address the scheduling design. Furthermore, results also present connections to classical information theoretic problems such as wire tapped channel communication and rate distortion, now present novel applications.

Chi-Yin Chow et al [6], proposed a privacy-preserving location monitoring system concept for wireless sensor networks. In this literature, the author designed two in network location anonymization algorithms, like as resource and quality-aware algorithms which will be preserve personal location privacy, while at enabling this approach to provide location monitored service in wireless sensor networks. Both these algorithms depend on the k-anonymity privacy approach that requires a person is indistinguishable among k persons. In this system, sensor nodes execute the location anonymization algorithms which is provide k-anonymous aggregate locations, in which each aggregate location is a cloaked area A with the number of monitored objects, N, located in A, where N _ k, for the system. The second one is resource-aware algorithm aims to minimize communication and computational cost, other side the quality-aware algorithm aims to minimize the size of cloaked areas in order to create more accurate aggregate locations.

III. OBJECTIVES

In particular the main objective for this works is described the network and adversarial assumption. In network model, communication is assumed to take place in a network of energy constrained sensor nodes. Nodes are deployed to sense events and report them with minimum delay. Furthermore, the network is assumed to be deployed in an unreachable environment and, therefore, the conservation of nodes energy is a design requirement. In adversary model there are external, passive and global adversary are to be considered. For achieving source anonymity in sensor network is to refrain from event-triggered transmission in the availability of global adversaries and this is the proposed methodology for wireless sensor network.

IV. PROPOSED WORK

In this work, sometimes at the time of transmitting the "description" of a sensed event it can be achieved via encryption fashion, hide the timing of transmission of sensed events and spatial information of reported events cannot be get via cryptographic approaches. The source anonymity problem has been addressed on two different types of adversaries, namely, global adversaries and local adversaries. In a global adversary, it has full spatial view of the network, and it can quickly detect the origin or source and time of the event-triggered transmission. So to solve these problems in the Statistical Source Anonymity (SSA) in wireless sensor networks is the study of techniques that saves the sensed events to 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.

In the SSA Systems, here below are some modules which are in the execution mode. When system is the starting condition, and interval indistinguishability, Quantitative Measure Module, these modules are executing.

4.1 Neighbor Discovery

In this section, the source node searched for the other node which is in the range, and that is said to be neighbor node. After this process it will transmits the sensed events from source node to neighbor node. Here X axis, and Y axis dimensions would have to be put up to manage all the sensor nodes. And here Z axis dimensions will not be put because the only 2D view is available, so put Z dimension as zero.

4.2 Interval Indistinguishability

In this approach, at a particular time which is in milliseconds (msec), nanoseconds (nsec) it will send both the fake and real sensed events by the node. To understand this concept, we taken an example as below,

Let 'I_F' denote a time interval without any real event transmissions, and 'I_R' denotes a time interval with real event transmissions, The two time intervals are said to be statistically indistinguishable if the distributions of inter-transmissions timed during these two intervals cannot be distinguish with significant confidence.

4.3 Quantitative Measure

In this scenario, the mathematical formula has been given and that formula decides the time interval at which both fake and real sensed events have to be sent.

And then the adversary is unable to infer when an interval starts or when it ends. This is mandatory because an adversary with the knowledge that a node is transitioning from one interval to another will infer that either real events have started to arrive or stopped from arriving.

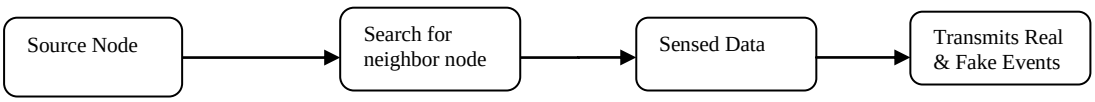

Figure 2: Flow of proposed System

These above mentioned scenarios are makes the system large factor in wireless Sensor networks and with the security point of view it also gains an enormous importance.

V. CONCLUSION

In this paper, provides a statistical approach which will be based on binary hypothesis testing for modeling, analyzing, and evaluating statistical source anonymity in wireless sensor networks. Here introduced the idea of interval indistinguishability to model source location privacy. And the current scenario for design statistically anonymous systems introduced correlation in real intervals and fake intervals are uncorrelated. The problem of detecting source information to the statistical problem of binary hypothesis testing with some parameters, and proposed a solutions to improve the anonymity concept against correlation tests. The future scope to this work is to include mapping the problem of statistical source anonymity to coding theory in order to design an efficient system that satisfies the idea of interval indistinguishability.

REFERENCES

[1] Basel Alomair, Andrew Clark, Jorge Cuellar, and RadhaPoovendran, "*Toward a Statistical Framework for Source Anonymity in Sensor Networks*", IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013.

[2] Mauro Conti, JeroenWillemsen, and Bruno Crispo, "*Providing Source Location Privacy in Wireless Sensor Networks: A Survey*" IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013.

[3] Wei Tan, KeXu, Dan Wang, "*An anti-tracking source-location privacy protection protocol in WSNs based on path extension*" IEEE Internet of Things Journal, 2013.

[4] Yun Li, JianRen, and JieWu,"*Quantitative Measurement and Designof Source-Location Privacy Schemes for Wireless Sensor Networks*" IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 7, July 2012.

[5] Chi-Yin Chow, Mohamed F. Mokbel, andTian He, "*A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks*" IEEE Transactions on Mobile Computing, Vol. 10, No. 1, January 2011.

[6] ParvVenkitasubramaniam, Ting He, Lang Tong, and Stephen B. Wicker, "*Toward an Analytical Approach to Anonymous Wireless Networking*" Security in Mobile Ad Hoc and Sensor Networks, February 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] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "*Statistical Framework for Source Anonymity in Sensor Networks*," Proc. IEEE GlobeCom, 2010.

[9] Q. Gu, X. Chen, Z. Jiang, and J. Wu, "*Sink-Anonymity Mobility Control in Wireless Sensor Networks*," Proc. IEEE Fifth Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WiMob '09), pp. 36-41, 2009.

[10] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "*An Efficient Privacy-Preserving Scheme against Traffic Analysis Attacks in Network Coding*," Proc. IEEE INFOCOM, pp. 19-25, 2009.

[11] Q. Gu, X. Chen, Z. Jiang, and J. Wu, "*Sink-Anonymity MobilityControl in Wireless Sensor Networks*," Proc. IEEE Fifth Int'l Conf.Wireless and Mobile Computing, Networking and Comm. (WiMob '09),pp. 36-41, 2009.

[12] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "*Random-WalkBased Approach to Detect Clone Attacks in Wireless SensorNetworks,*" IEEE J. Selected Areas in Comm., vol. 28, no. 5, pp. 677-691, June 2010.

