International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

Source Location Privacy Preservation In Wireless Sensor Networks

Pranil M.Kale[1], Gulshan I[2]. Nimbekar[3], Nikhil Shankhadarwar[4]
[1,2,3,4] Department of Computer Science & Engineering
College of Engineering & Technology, NIT,Nagpur.

Abstract:- Many attackers use the nodes location information for security threats in network, as every sensor node in network is having its own location. An attacker tries to get location information of source or receiver. Wireless sensor networks (WSNs) are group of collection of sensor nodes which are collaboratively communicate with each other for information sharing. The sharing of information is done between source sensor node and sink sensor node using the routing protocols. The major constraint of this network is the security. Thus we need to have source location privacy methods in WSN to prevent such threats from the network. Source privacy preservation is also called source anonymity and recent time this attracts many researchers interests. The attacker or unauthorized sensor node not able to get events location information through the current network traffic is called as source anonymity problem. Recently we have studied efficient method for source anonymity in WSNs. In most of real life applications of WSNs, sensor networks are having the location information about various events and this information needs to secure or anonymous. In that method the statistical framework is presented, this is based on the binary hypothesis testing for modeling, analyzing, and evaluating statistical source anonymity WNS. The concept of notion of interval in distinguish ability in order to model source anonymity, however this method fails to satisfy the notion of interval in distinguish ability practically. Therefore, in this paper we are further extending this method address such issues and practically prove its efficiency, we proposed a modification to existing solutions to improve their anonymity against correlation tests.

Key-Words: - Pairwise Key Establishment, Advanced Encryption Standard (AES), Sensor Network Security, Security communication overhead.

I. INTRODUCTION

Recently we have studied in Toward a Statistical Framework for Source Anonymity in Sensor Networks. In most of applications the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic, Security of wireless sensor networks, with variety of techniques based on different adversarial assumptions it introduces the notion of "interval in distinguish ability" and provides a quantitative measure to model anonymity in wireless sensor networks; second, it maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. In which 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. Transform 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. In Proposed system propose a quantitative measure to evaluate statistical source anonymity in sensor networks.

Sensor networks are deployed to sense, monitor, and report events of interest in a wide range of applications including, but are not limited to, military, health care and animal tracking. 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. The locations of the combat vehicle at different time intervals can be revealed to an adversary observing nodes transmissions.

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. While transmitting the "description" of a sensed 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. 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.

In the existing literature, the source anonymity problem has been addressed under two different types of adversaries, namely, local and global adversaries. A local adversary is defined to be an adversary having limited mobility and partial view of the network traffic. Efficient power saving scheme and corresponding algorithm must be developed and designed in order to provide reasonable energy consumption and to improve the network lifetime for wireless sensor network systems. The cluster-based technique is one of the approaches to reduce energy consumption in wireless sensor networks. In this article, we propose a optimize energy clustering algorithm to provide efficient energy consumption in such networks. The main idea of this article is to reduce data transmission distance of sensor nodes in wireless sensor networks by using the uniform cluster concepts. In order to make an ideal distribution for sensor node clusters, we calculate the average distance between the sensor nodes and take into account the residual energy for selecting the appropriate cluster head nodes. The lifetime of wireless sensor networks is extended by using the uniform cluster location and balancing the network loading among the clusters. Simulation results indicate the superior performance of our proposed algorithm to strike the appropriate performance in the energy consumption and network lifetime for the wireless sensor networks.

WSN is nothing but the group of number of small sensor wireless devices which are constrained for limited resource. These devices are also called as motes. In addition to this, WSN consisting of one or few general purpose computing devices referred to as base stations (or sinks). The basic use of WSN is to perform the monitoring of physical phenomenon for example light monitoring, temperature monitoring, barometric monitoring etc over the geographical area of WSN deployment. Each sensor node in WSN is having the functionalities such as battery, processing unit and sensors. Each sensor node is having limitations of battery power which is means WSN is resource constrained. On the other hand, the base stations in WSN are nothing but laptops capabilities therefore those are not power constrained. The role of base station is bridge the communication gap between the other networks and WSN. The real time applications of WSNs are military applications, health applications, commercial applications, temperature monitoring etc.

II. Problem Formulation

- Many attackers use the nodes location information for security threat in network, as every sensor node in network is having its own location.
- Thus we need to have source location privacy methods in WSN to prevent such threats from the network.
- Source privacy preservation is also called source anonymity and recent time this attracts many researchers interests.
- A wireless sensor network that is composed of low-power, low-cost sensor nodes these nodes have limited power supply, storage space, and computational capability.
- Due to the constrained resources, computationally expensive and energy intensive operations are not favorable for such systems.

III. PROJECT WORKFLOW

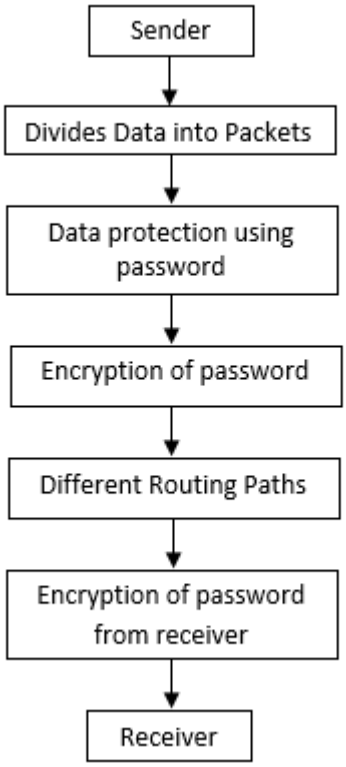

Fig. 1. Workflow of Project

REFERENCES

i. Basel Alomair Member, IEEE, Andrew Clark, Student Member, Jorge Cuellar, and Radha Poovendran, Senior Member, IEEE, "Toward a Statistical Framework for Source Anonymity in Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

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

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

iv. 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.

