ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Emulated Source/Sink Location Privacy Algorithm [ESLPA] for Secure Node and Sink in WSN

D. Gopinath[1] , P. Ramesh[2]

Assistant Professor, Dept. of Computer Science, Kongu Arts and Science College, Erode, Tamilnadu, India.[1]

Assistant Professor and Head, Dept. of Computer Science, Kongu Arts and Science College, Erode, Tamilnadu, India [2]

ABSTRACT: A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices. Sensors are used to cooperatively monitor physical or environmental conditions. Sensor network is equipped with a radio transceiver or other wireless communications device. The sensor networks are deployed with consideration of sensing and transmission coverage factors.

Data confidentiality is the most important issue in network security. The objective of confidentiality is required in sensors environment to protect information travelling among the sensor nodes of the network. Sensor network security protocols provide confidentiality for the messages. Object location and data sink information are the sensitive elements in the sensor network. In certain 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 known as 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.

To solve source anonymity problem, nodes are required to transmit fake messages even if there is no detection of real events. The concept of "interval distinct" is proposed to distinguish between real and fake transmissions by means of statistical analysis. The source anonymity is mapped to the statistical problem of binary hypothesis testing. The proposed system integrates the location privacy and data security process for the wireless sensor network. Emulated Source/Sink Level Privacy Algorithm (ESLPA) is proposed to improve Node and Sink Level Privacy.

KEYWORDS: WSN, interval distinct, ESLPA, Node Level Privacy, Sink Level Privacy.

I. INTRODUCTION

Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through infrastructureless ad-hoc wireless network. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes. Akyildiz et al. [3] argued that the cost of a sensor node should be much less than one dollar in order for sensor networks to be feasible. Therefore, most sensor nodes are resource restrained in terms of energy, memory, computation, and communication capabilities. Normally sensor nodes are powered by batteries, and recharging batteries are infeasible in many circumstances. Energy consumption becomes a key consideration for most sensor network protocols. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. Generally, adversaries are assumed to be able to undetectably take control of a sensor node and extract all secret data in the node. Furthermore, the scale of sensor networks is considerably large, and the network topology is dynamically adjusted, because some nodes may die out of running out of energy or failure, and new nodes may join the network to maintain desirable functionality. At last, sensor networks use insecure wireless communication channel and lack infrastructure.

DOI: 10.15680/IJIRCCE.2015. 0312079

SECURITY REQUIREMENTS

WSN can be considered as a highly distributed database with wireless links. Security goals for distributed databases are very well studied. The data should be accessible only to authorized users (confidentiality), the data should be genuine (integrity), and the data should be always available on the request of an authorized user (availability). All these requirements also apply to WSNs and their users.

Data confidentiality is the most important issue in network security. The objective of confidentiality is required in sensors environment to protect information travelling among the sensor nodes of the network or between the sensors and the base station from disclosure. With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe.

The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

Authentication in sensor networks is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender or not. This authentication is needed during the clustering of sensor nodes in WSN. The receiver can trust the data sent by the nodes in that group after clustering. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Secure management is needed at base station, clustered nodes, and protocol layer in WSN. Because security issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management. Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. Another important issue is the availability factor of the nodes or the transmission media. The network should remain operational all the time. It must have some redundancy to counter link failures and have the capability to survive against different attacks.

II. RELATED WORK

PRIVATE QUERIES IN LOCATION BASED SERVICES:

Privacy is not protected by replacing the real user identity with a fake one, because, in order to process location-dependent queries, the LBS [10] need the exact location of the querying user. An attacker, which may be the LBS itself, can infer the identity of the query source by associating the location with a particular individual. This can be easily performed in practice, with the help of a public telephone directory, for instance, which contains subscribers' addresses.

The framework is to support private location dependent queries, based on the theoretical work on Private Information Retrieval (*PIR*) [8]. This framework does not require a trusted third party, since privacy is achieved via cryptographic techniques.

There are two privacy issues in location-dependent queries:
(i) The user must hide his identity (e.g., username, IP address, etc). This is orthogonal to the problem and can be achieved through a widely available anonymous web browsing service (that service does not learn the location of *u*).
(ii) The user must hide his location. Similar to previous research on spatial *K*-anonymity, this PIR framework focuses on this issue. The advantages of the approach are:

- PIR does not disclose *any* spatial information.
- PIR protects against correlation attacks.
- PIR reduces significantly the identification probability.
- PIR does not require any trusted third party
- PIR reduces the number of disclosed POI.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

PROTECTING LOCATION PRIVACY IN LARGE-SCALE WIRELESS SENSOR NETWORKS:

In a wireless sensor network, an adversary equipped monitoring antenna can easily overhear packets, which may facilitate identifying the directions of packet flows and trace to the sink or source nodes. In order to defend the location privacy of the sink and source nodes, a Location Privacy Support Scheme (LPSS) [9] was proposed.

In order to secure the locations of the sink and source, a new scheme was used, called the location privacy support scheme (LPSS), to produce broadly diverse paths with tunable delivery delay. Under the similar delivery delay (or energy cost), the paths produced by LPSS can support longer safe time than other approaches. With the increase in distance between sink and source node, the protection strength of LPSS increases exponentially.

The performance of LPSS was evaluated through simulations based on three criteria: delivery delay, strength of privacy protection and energy cost, which will be defined later. These methods are compared our methods with single-path routing and two other location privacy protection schemes: Phantom routing (PhR) in [5] and location privacy routing (LPR) in [6]. Single path routing is assigned as the baseline routing scheme. When evaluating the strength of privacy protection, the study was made about the scenario against patient hunter (without fake packets injection) and then come into the scenario against impetuous attacker (where fake packets are used).

PROTECTING RECEIVER-LOCATION PRIVACY IN WIRELESS SENSOR NETWORKS

Privacy in sensor networks may be classified into two categories [5]: content privacy and contextual privacy. Threats against content privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a sensor network. This type of threats is countered by encryption and authentication. However, even after strong encryption and authentication mechanisms [1], [4] are applied, wireless communication media still exposes contextual information about the traffic carried in the network. For example, an adversary can deduce sensitive information from a sensor network by eaves dropping the network traffic and analyzing the traffic patterns. In particular, the location information about senders/receivers may be derived based on the direction of wireless communications. In paper was focus on the protection of location privacy for the receiver in sensor networks.

SECURE IMPLICIT GEOGRAPHIC FORWARDING (SIGF)

A. D. Wood et al. [2] have proposed a configurable secure routing protocol family called Secure Implicit Geographic Forwarding (SIGF) for WSNs. The SIGF is based on the Implicit Geographic Forwarding (IGF) protocol in which a packet is forwarded to the node that lies within the region of 60◦ sextant, centered on the direct line from the sender to the destination. The SIGF protocol provides some aspects of networks privacy such as data, route and location privacy. However it does not provide identity privacy. Another, limitation of the SIGF protocol is that, when there is no trusted node within a forwarding area (assuming 60◦ sextant), it will forward the packet to a un-trusted node. So, the reliability of the path is affected.

GREEDY RANDOM WALK (GROW)

Y. Xi et al. [7] proposed a Greedy Random Walk (GROW) scheme for preserving location of the source node. This scheme works in two phases. In a first phase, the sink node will set up a path through random walk with a node that act as a receptor. Then the source node will forward the packet towards the receptor in a random walk manner. Once the packet reaches at the receptor, it will forward the packet to the sink node through the pre-established path. Here receptor is acting a central point between the sink and the source node for every communication session. A criterion of selecting a trustworthy receptor is essential that is not defined.

III. PROBLEM FORMULATION

PROBLEM STATEMENT

Generally, countermeasures to the threats in WSNs should fulfil the following security requirements:

- Availability, which ensures that the desired network services are available whenever required.

- Authentication, which ensures that the communication from one node to another node is genuine.
- Confidentiality, which provides the privacy of the wireless communication channels.
- Integrity, which ensures that the message or the entity under consideration is not altered.
- Non-reputation, which prevents malicious nodes to hide or deny their activities.
- Freshness, which implies that the data is recent and ensures that no adversary can replay old messages.
- Survivability, which ensures the acceptable level of network services even in the presence of node failures and malicious attacks.
- Self-security, countermeasures may introduce additional hardware and software infrastructures into the network, which must themselves be secure enough to withstand attacks.

OBJECTIVES

- The aim of the thesis is to integrate the location privacy and data security process for the wireless sensor network.
- The wireless sensor security system is designed to secure the query request and response models.
- The proposed system integrates the security and privacy methods for the data query process.
- Confidentiality and data integrity techniques are used to secure both data request and response values.
- Fake query model is used to handle the intruders.
- Statistical anonymity in sensor networks is modeled to distinguish between real and fake transmissions by means of statistical analysis.
- Region based query model is used to improve location privacy.

IV. NODE LEVEL AND SINK LEVEL PRIVACY

The wireless sensor security system is designed to secure the query request and response models. The system considers a homogeneous network model. In the homogeneous network model, all sensors have roughly the same computing capabilities, power sources, and expected lifetimes. This is common network architecture for many applications today and will likely continue to be popular moving forward. It is well studied and provides relatively straightforward analysis in research as well as simple deployment and maintenance in the field. This research can be applied to a variety of sensor platforms. Each sensor has a limited lifespan and the network must be designed to preserve the sensors' power reserves. It has been demonstrated that sensors use far more battery power for transmitting and receiving the data. The system integrates the security and privacy methods for the data query process. Confidentiality and data integrity techniques are used to secure both data request and response values. Fake query model is used to handle the intruders.

In certain 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 known as the source anonymity problem. The first step toward 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 detection of events of interest (real events will be used to denote events of interest). When a real event occurs, its report can be embedded within the transmissions of fake messages. Thus, given an individual transmission, an observer cannot determine whether it is fake or real with a probability significantly higher than 1/2, assuming messages are encrypted.

In this approach, there is an implicit assumption of the use of a probabilistic distribution to schedule the transmission of fake messages. However, 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 knowledge of the fake transmission distribution, statistical analysis can be used to identify outliers (real transmissions) with a probability higher than 1/2. 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.

V. PROPOSED FRAMEWORK FOR SSA

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.

INTERVAL DISTINCT

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.

Consider now an adversary observing a sensor network over multiple time intervals. Assume that, during a given time interval, the adversary is able to notice a change in the statistical behavior of transmission times of a certain node in the network. This distinguishable change in the transmission behavior of the node can be indicative of the existence of real activities detected and reported by that node during that interval, even if the adversary was unable to distinguish between individual transmissions.

Consequently, in many applications, modeling source anonymity in sensor networks by the adversary's ability to distinguish between individual transmissions is insufficient to guarantee location privacy. It must be the case that an adversary monitoring the network over multiple time intervals, in which some intervals contain real event transmissions and the others do not, is unable to determine, with significant confidence, which of the intervals contain the real traffic.

Interval versus Event Distinct

The relation between the traditional anonymity notion (i.e., individual event distinct) and the proposed anonymity notion (i.e., interval distinct) are. First, observe that as the length of intervals decreases or the transmission rate is sparse, interval distinct approaches event distinct. If each interval consists of a single transmission, interval distinct is equivalent to event distinct.

However, in the more general scenario, in which intervals contain more than a single transmission, interval distinct implies distinct of individual transmissions. To see this, assume a system satisfying interval distinct but does not satisfy individual event distinct. Since real and fake transmissions are distinguishable, given a fake interval and a real interval, the real interval can be identified as the one with the real transmission; a contradiction to the hypothesis that the system satisfies interval distinct. That is, if intervals are indistinguishable, then individual events within them must also be indistinguishable.

In fact, the notion of interval distinct is strictly stronger than the traditional notion individual event distinct. That is, while interval distinct implies individual distinct, the converse is not true in general.

Mapping Statistical Source Anonymity to Binary Hypothesis Testing

In binary hypothesis testing, given two hypothesis, H_0 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 distinct, given an interval of inter-transmission times, the goal is to decide whether the interval is fake or real (i.e., consists of fake transmissions only or contains real transmissions).

VI. EMULATED SOURCE/SINK LOCATION PRIVACY ALGORITHM [ESLPA]

Emulated Source/Sink Level Privacy Algorithm (ESLPA) is the combination of Node Level Privacy technique and Sink Level privacy technique. By using these techniques**,** the network traffic and fake sink should be avoided. From this, energy consumption should be reduced compared to other various schemes.

NODE LEVEL PRIVACY

Periodic Collection technique is proposed to provide Node level privacy to monitor objects in sensor networks.

Periodic Collection

Previous schemes fail against a global eavesdropper. The primary reason is that the presence of a real object will change the traffic pattern at the place where the object resides. This allows the global eavesdropper to easily find out where the change happens. An intuitive solution is to make the traffic pattern independent of the presence of real objects. To achieve this, every sensor node independently and periodically send packets at a reasonable frequency regardless of whether there are real data to send or not. Specifically, each sensor node has a timer that triggers an event every Δ second, as well as a first-in-first-out (FIFO) queue of size q for buffering received packets that carry real data reports. When the timer fires, the node checks if it has any packets in its queue. If so, it dequeues the first packet, encrypts it with the pairwise key it shares with the next hop, and forwards it to that node. Otherwise, it sends a dummy packet with a random payload that will not correctly authenticate at the next hop. Since every sensor node only accepts the packets that correctly authenticate, dummy packets do not enter the receiver's queue. When the queue at a sensor node is full, it will stop accepting new packets.

SINK-LEVEL PRIVACY

The privacy-preserving routing technique is proposed, backbone flooding is used for sink level privacy in sensor networks. The backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks. This technique provides trade-offs between privacy, communication cost, and latency.

Backbone Flooding

In backbone flooding, the packets are sent to a connected portion of the network, the backbone, instead of sending them directly to a few sinks. The packets are only flooded among the backbone members, the sensors that belong to this backbone. As long as the real sinks are located in the communication range of at least one backbone member, they can receive packets from any source in the field. Clearly, for a global eavesdropper, the sink could be anywhere near the backbone. The backbone is created soon after the network is deployed and that the adversary does not eavesdrop until the backbone is created.

The main component of backbone flooding is the construction of the backbone. Existing studies have focused on finding the minimal number of sensors that are needed to flood a packet so that the entire network can receive it. The focus on this thesis is, need to flood the packets to cover an area large enough to achieve the desired level of location privacy. In backbone flooding, a backbone consisting with |L| members, such that each sink is within the range of at least one backbone member. Given |L|, the backbone formed should cover as large an area as possible for maximum location privacy.

Every new sensor v added to the set L will send an election message to find the number of uncovered sensors each neighbor can cover. If $\max_v(m)$ outputs a valid sensor ID and the coverage of this node, the ID of this node will be added to L. The newly added sensor will then execute the same algorithm. If $\max_v(m) = \perp$, v will collaborate with existing nearby backbone members to find a usable sensor. The backbone is a tree structure with backbone members as the tree nodes. During the collaboration, the sensor will need to get information from its parent to find a node that can cover at least m nodes. This collaboration could continue to next level of ancestors if such a node is not known to the immediate parent. This backtracking process continues until a sensor meeting the required constraints is found. If a sensor that can cover at least m uncovered sensors is unavailable, a sensor that covers the maximum number of uncovered sensors is used.

Algorithm **Backtrack Procedure**

```
procedure BACKTRACK(Coverage, Id,m)
    ResultId$\leftarrow$ Id
    Max $\leftarrow$ Coverage
    LocalMaxId$\leftarrow$ -1
    CollectCoverageInfo(GetMyId(),NULL)
    (LocalMaxId,Max) $\leftarrow$MaxId(m)
    if Max $\geq$ m then
        return LocalMaxId, Max
    else if Max < Coverage then
        ResultId = LocalMaxId
        Max = Coverage
    end if
    for EachUnvisitedNeighborBKMember do
        (Id,Coverage) = Backtrack(Max, ResultId,m)
        if Coverage $\geq$ m then
            ResultId = Id
            Max = Coverage
            break
        else if Coverage > Max then
            Max = Coverage
            ResultId = Id
        end if
    end for return ResultId,Max
end procedure
```

The beginning and termination of the backtracking process depends on the value of m. A value of $m \leq 1$ would mean that backtracking would start only if v cannot find any neighbor that can cover at least one uncovered sensor. If m has a value greater than the number of neighbors any sensor could have, then the backtracking process would ensure that the sensor that covers the maximum number of uncovered sensors is selected. Intuitively, this would mean that an increase of m would help in covering more sensors with the help of fewer backbone members.

VII. PROPOSED FRAMEWORK FOR SSA

The wireless sensor network query system is designed to handle query requires and response with security and privacy. The privacy ensured model uses the Node level and Sink level based privacy preservation methods for data query process. The data request is secured and protected with its location details. All the user query values are secured with the request details. The ESLPA is emulated with data request and response based security methods. The query response is secured with confidentiality and integrity methods. The signature values are used to verify the data request and response attacks. The privacy is ensured using the fake query transmission process. The wireless sensor network data query system is tested with different node count and different query type methods. The sink level query and node level query values are used for the data retrieval process. In the sink level query model all the data requests are transferred from the base station to the sink node. The sink node redirects the received query value to its associated to the sensor nodes. But in the case of node level query the data request is directly transferred to the source node through the intermediate sensor nodes. The privacy is provided with fake query values. The intruders can't able to identify the exact query value and its source.

The system is tested with two performance metrics. They are energy consumption and traffic overhead levels. The energy consumption reduction rate is calculated for the both Existing and ESLPA methods.

Nodes	Exising %	ESLPA %
10	11	22
20	14	26
30	18	29
40	21	33
50	23	36

Table 1. Energy Saving Analysis

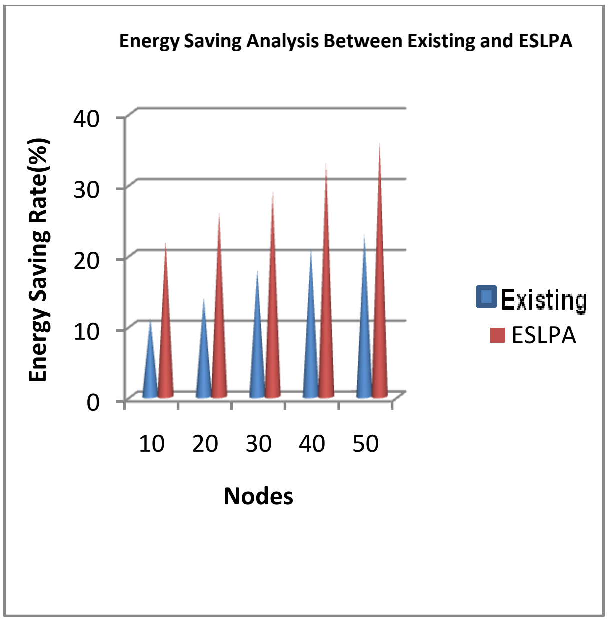

Fig. 2. Energy Consumption by Each Node

The energy consumption reduction results are produced in Table 1. The comparison analysis is shown in figure 1. The result shows that energy consumption of ESLPA is reduced 35% than the SLPA method.

Nodes	Existing	ESLPA
10	11	6
20	15	8
30	19	11
40	26	14
50	35	19

Table 2. Traffic Overhead analysis

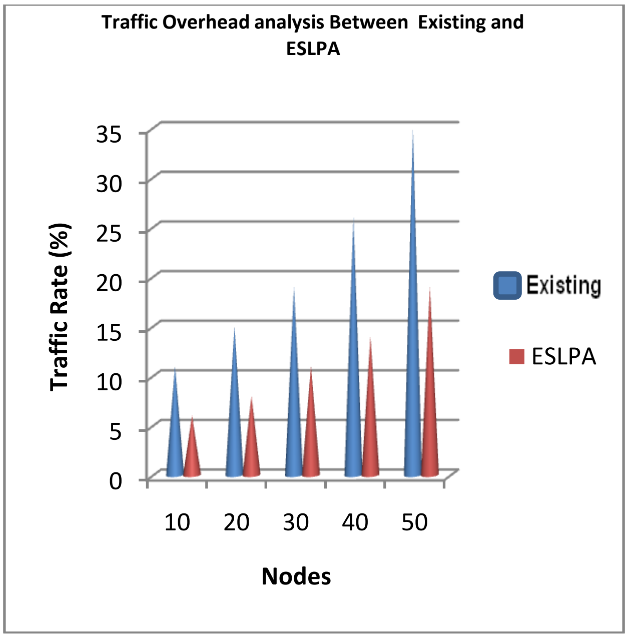

Fig. 2. Energy Consumption by Each Node.

The traffic rate overhead is reduced in the ESLPA model. The traffic overhead rate is analysed in the Table 2. The comparison analysis is shown in figure 2. The overhead is reduced 40 % in ESLPA than the Existing model.

VIII. Conclusion and Future Work

Sensor networks are constructed to capture environment information. Data centres collect information from sensor devices. Data security is integrated with the location privacy scheme to improve security on data transmission in wireless sensor network.

The problem of source anonymity is avoided by transmitting fake messages and the concept of interval distinct is used to find real and fake message or query.

Node and Sink Level Privacy is improved by using Emulated Source/Sink Level Privacy Algorithm [ESLPA]. The periodic collection technique is used for Node Level Privacy and the Backbone Flooding technique is used for Sink Level Privacy. In ESLPA, Sensitive location and data values are protected by using these techniques.

The sensor network security and privacy management system can be enhanced with the following features.

- The system can be adapted to support data caching methods for query process.
- The system can be adapted to handle data monitoring under mobile sensor environment.
- The data query model can be improved to support continuous data monitoring process.
- The system can be enhanced to support aggregation query model and top-k query models.

References

1. A. D. Wood, L. Fang, J. A. Stankovic, and T. He, “SIGF: a family of configurable, secure routing protocols for wireless sensor networks”, In Proc. of 4th ACM workshop on Security of ad hoc and sensor networks, pages 35–48, Alexandria, Virginia, USA, 2006.
2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci”A survey on sensor networks”, IEEE Communications Magazine, 2002.
3. L. Eschenaur and V. Gligor, “A key-management scheme for distributed sensor networks”, Proc. of 9th ACM conference on Computer and Communications Security, 2002.
4. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source location privacy in sensor network routing”, Proc. of 25th IEEE International Conference on Distributed Computing Systems (ICDCS), 2005.

5. Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting Receiver-Location Privacy in Wireless Sensor Networks”, In 26th IEEE International Conference on Computer Communications (INFOCOM 2007), pages 1955–1963, May 2007.
6. Y. Xi, L. Schwiebert, and W. Shi, “ Preserving source location privacy in monitoring-based wireless sensor networks”, In Proc. of IPDPS 2006, Rhodes Island, Greece, Apr 2006.

BOOKS

7. Andrew S. Tanenbaum, “Computer Networks”, Fourth Edition, Prentice Hall, 2003
8. B. Schneier, “Applied Cryptography”, Second Edition, John Wiley & Sons, 1996.
9. David Groth, “Network+ ™”, Study Guide, Third Edition, SYBEX, Inc., Alameda, CA, 2002
10. P. Glover and M. Grant, “Digital Communications”, 2nd edition, Person Education, 2004.

WEB SITS

11. http://www.libelium.com/wireless_sensor_networks_to_detec_forest_fires/
12. www.ieee.org
13. www.springerlink.com
14. www.infomit.org

BIOGRAPHY

Mr.D.Gopinath received his B.Sc, M.Sc and M.Phi degree in Computer Science from the Bharathiar University. He is currently working as a Assistant Professor in Kongu Arts and Science College. He had presented papers at various National and international conferences. His area of interest includes Wireless sensor Network Security, Network Security, Ad Hoc Network, especially design and implementation of security metrics.

Mr.P.Ramesh, Head, Department of Computer Science in Kongu Arts and Science College, Erode. He received the B.Sc Degree under Bharathiar University, M.Sc Degree under Bharathidasan University and M.Phil under Manonmanium Sundaranar University – Tirunelvelli. Currently he is doing his Ph.D under Bharathiar University. He had presented more than 20 papers in National and international conference