ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Performance Based Location Privacy in Sensor Networks against a Global Eaves Dropper

Mr.K.Venkatesh[*1], Mrs.A.Kannammal[2]

[*1] Student, Department of CSE, Jayam College of Engineering & Technology, Dharmapuri-636813, Tamil Nadu, India

[2] Asst. Professor, Department of CSE, Jayam College of Engineering & Technology, Dharmapuri-636813, Tamil Nadu, India

venkanthi@gmail.com

Abstract

Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a short region. However, an energetic attacker, the global eavesdropper, is realistic and can defeat these existing techniques. This proposal first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. The project then proposes two approach to provide location privacy to monitored objects (source-location privacy)—periodic collection and source simulation—and two approach to provide location privacy to data sinks (sink-location privacy)—sink simulation and backbone flooding. These procedures provide understanding between privacy, communication outlay, and latency. Through investigation and simulation, it is scheduled to demonstrate that the proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.

Keywords: Global Eavesdropper, Mobile Computing.

Introduction

The Term "Mobile Computing" was introduced not long after the concept of "Cloud Computing" introduced in mid-2007. It has been attracting the minds of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, of mobile users as a new equipment, to achieve rich experience of a variety of mobile services at low cost, and of researchers as a favourable solution for green IT. Using diverse phones from everywhere in the world is not activity that could be called mobile computing - because there is no computing involved.

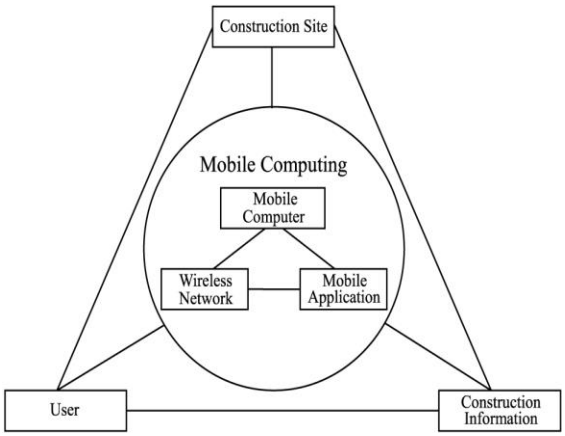
Dragging around a laptop and working with it without being able to set up a connection to the "home base" through a computer network is neither mobile computing in a strong sense; one must be able to communicate with "home base" and people in other organizations.

A. Architectures of Mobile Computing

Does mobile computing need some devices to be delayed around by the people? Not essentially, an organization with proper access devices could be offered to travelling people - in the same manner as telephones are offered in hotels, airports, etc, still cheap small portable devices like PDAs, laptops, and devices like Nokia Communicator are historically fundamental for the idea of mobile computing.

Another important development are the advances in computer networking organization that make global connectivity possible. One great development is the Internet as a global network organization, but in this context particularly the wireless technologies are very important. Wired portable devices can be connected to the network organization only in certain locations for a certain period of time. Communication activity of a nomad is spatially and temporally limited. Wireless portable devices, especially those functional with radio transmitter/receiver avoid the above problem to a great extent.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852



B. Applications of Mobile Computing

The importance of Mobile Computers has been tinted in many fields of which a few are described below:

1. For Estate Agents

It can work either at home or out in the field. With mobile computers it can be more expensive. Obtain current real estate knowledge by accessing multiple listing services, which can do from home, office or car when out with clients. Provide clients with immediate response regarding specific homes, and with faster loan approvals, since applications can be yielded on the spot.

2. Emergency Services

Ability to receive data on the move is vital where the emergency services are involved. Data regarding the address, type and other details of an incident can be dispatched quickly, via a system using mobile computers, to one or several suitable mobile units, which are in the locality of the incident.

3. In courts

Defence counsels can take mobile computers in court. When the testimonials, counsel references a case which are not familiar, use the computer to get direct, real time access to on-line official database services, where can gather information on the case and related precedents. Therefore mobile computers passes immediate access to a wealth of information, making people better learned and prepared.

4. In Industry

Managers can use mobile computers and critical presentations to major customers. Access the latest market share information. Communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can control competitive advantages.

5. Credit Card Verification

At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for business, the intercommunication demand in the middle of the bank central computer and the POS terminal, in order to effect authentication of the card usage, can take place promptly and securely over cellular channels using a mobile computer unit. This can speed up the operation process and relieve congestion at the POS terminals.

6. Electronic Mail/Paging:

Usage of a mobile unit to send and read emails is a very useful asset for any business unique, as it allows him/her to keep in touch with any colleagues as well as any urgent developments that may alter their work. Right to use of the Internet, using mobile computing technology, admit the particular to have vast arrays of knowledge at his/her fingertips. Paging is also authentic here, giving even more intercommunication capability in the middle of individuals, using a single mobile computer device.

7. Mobile Computing Risks Are Rising:

Mobile computing devices for the flexibility and convenience are provide, but mobility presents significant challenges for IT administrators charged with keeping their companies' data and networks secure-particularly as mobile devices and networks have grown more sophisticated and ubiquitous. While these challenges make managing security on mobile devices a trickier proposition, there are ways supervisors, can help plug the holes that mobile devices have a way of opening in your company's security organization .

However, there's no one-size-fits-all resolution, and administrators will have to take a long, hard look at each and every user-and gadget-accessing corporate data to ensure that all the gaps are filled. The more portable a device, the easier it is to lose whether by accident or wicked intent. In any case, the digital booty these machines bear can range from one person's list of bank passwords to a spreadsheet containing the Social Security numbers and other personal information of tens of thousands of students-as the University of California, Berkeley, proven a few months back when such a list left the campus on a pilfered notebook computer.

Often more crucial than the data stored on mobile devices is the role that these systems play as

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

gateways to an organization's network resources-a lost notebook, combined with a VPN client and saved password (which Windows XP's built-in VPN client allows by default) can be an open invitation into your corporate network.

C. Advantages Of Mobile Computing

- Quality Time, Maximum Time with Clients
- Better Data: Record Data Only Once
- True Portability: Go Anywhere
- Less Paperwork: Save Time, and Paper Too.

Helpful Hints

A Literature Review is an evaluative report of studies found in the literature related to the selected area. The review should designate, summarize, evaluate and clarify literature. It should give a theoretical basis for the research and helps to determine the nature of own research.

A. Location Privacy In Sensor Networks Against A Global Eavesdropper

Mehta.K, et al (2005) provides a formal model for the source-location privacy problem in sensor networks and examines the privacy characteristics of different sensor routing protocols. Examine two popular classes of routing protocols: the class of flooding protocols, and the class of route-planning protocols involving only a single path from the source to the sink. While investigating the secrecy performance of routing protocols, consider the tradeoffs between location-privacy and energy consumption.

Most of the current protocols cannot provide efficient source-location privacy while maintaining desirable system performance. Sensor networks promise to have a significant commercial impact by providing strategic and timely data to new classes of real time monitoring applications. One of the most notable challenges looming on the horizon that threatens successful deployment of sensor networks is privacy. Providing privacy in sensor networks is complicated by the fact that sensor networks consist of low-cost radio devices that employ readily available, standardized wireless communication technologies. As an example, Berkeley Motes hire a tuneable radio technology that is easily observable by spectrum analysers, while other examples be real sensor devices employing low power versions of 802.11 wireless technologies. As a result of the open-architecture of the underlying sensor technology, adversaries will be able to easily gain access to communications between sensor nodes either by purchasing their own low-cost sensor device and running it in a monitor mode, or by employing slightly more high-tech software radios capable of monitoring a broad array of radio technologies. Privacy may be defined as the guarantee that information, in its general sense, is obvious, or decipherable by only those who are intentionally meant to observe or decipher it. The phrase “in its general sense” is meant to imply that there may be types of information besides the message content that are associated with a message transmission.

Consequently, the secrecy threats that exist for sensor networks may be categorized into two broad classes: content-oriented security confidentiality threats, and contextual privacy threats. Content oriented protection and privacy threats are issues that arise due to the ability of the adversary to observe and manipulate the exact content of packets being sent over the sensor network, whether these packets correspond to actual sensed-data or sensitive lower-layer control information.

Although issues related to sensor security are important, many of the core problems associated with sensor security are on the road to eventual resolution due to an abundance of recent research by the technical community. Contextual privacy issues associated with sensor communication, however, have not been in detail addressed. In contrast to content-oriented security, the issue of contextual privacy is concerned with protecting the context associated with the measurement and transmission of sensed data.

For many scenarios, general contextual information surrounding the sensor application, especially the location of the message originator, are sensitive and must be protected. This is particularly true when the sensor network monitors valuable assets since protecting the asset’s location becomes critical. Many of the privacy techniques employed in general network scenarios are not appropriate for protecting the source location in a sensor network.

Due to the fact that the problems are different, and somewhat due to the fact that many of the methods introduce overhead which is too burdensome for sensor networks. One notable contest that arises in sensor networks is that the shared wireless medium makes it feasible for an adversary to locate the origin of a radio transmission, thereby facilitating hop-by-hop trace back to the origin of a multi-hop communication.

To address source-location privacy for sensor networks, this paper provides a formal model for the source-location privacy problem and examines the privacy characteristics of different sensor routing protocols. Introduce two metrics for

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

quantifying source-location privacy in sensor networks, the safety period and capture likelihood.

B. Wireless sensor networks: a survey

Akyildiz I, et al (2002) Recent advances in Micro-Electro-Mechanical Systems (MEMS) technology, wireless broadcasting, and digital electronics have enabled the occurrence of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate unthreads in short distances. These little sensor nodes, which depend on sensing, data processing, and communicating components, clout the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks stand for a significant improvement over constant sensors, which are deployed in the following two ways:

- Sensors can be positioned far from the actual fact, i.e., something known by sense perception. In this approach, huge sensors that use some complex techniques to distinguish the targets from environmental noise are required.
- Several sensors that perform only sensing can be adopted. The attitudes of the sensors and communications topology are carefully engineered. Transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

A sensor network is composed of a large number of sensor nodes, which are densely adopted either inside the phenomenon or very close to it. Position of sensor nodes need not be engineered or pre-determined. This allows random adopted in inaccessible terrains or disaster support operations. On the other hand, this also worth that sensor network protocols and algorithms must possess self-organizing capabilities. Another rare feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are incorporated with an on-board processor.

Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their development abilities to locally carry out simple computations and transmit only the required and partially processed data. The above portrayed features ensure a wide range of applications for sensor networks. Some of the function areas are health, military, and protection. For example, the functional data about a patient can be monitored remotely by a doctor.

While this is more convenient for the patient, it also grant the doctor to better understand the patient's current condition. Sensor networks can also be used to spot foreign chemical agents in the air and the water. To identify the type, attention, and location of pollutants. In essence, sensor networks will grant the end user with intelligence and a better understanding of the environment.

In future, wireless sensor networks will be an integral part of our lives, more so than the existent-day personal computers. Accomplishment of these and other sensor network applications require wireless ad hoc networking techniques. While many protocols and algorithms have been proposed for traditional wireless ad hoc networks, not well suited for the unique features and application requirements of sensor networks. To demonstrate this point, the differences between sensor networks and ad hoc networks are outlined below:

- The number of sensor nodes present in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network deviations very frequently.
- Sensor nodes mainly use relay communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are restricted in power, computational capacities, and memory.

Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors. Since large numbers of sensor nodes are densely adopted, neighbour nodes may be very close to each other. Hence, multi-hop interaction in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the diffusion power levels can be kept low, which is highly looked-for in covert operations.

Multi-hop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication. One of the most important bounds on sensor nodes is the low power consumption requirement. Sensor nodes carry restricted, generally one-off, power sources. Therefore, while fixed networks aim to achieve high Quality of Service (QoS) provisions, sensor network protocols must focal point, primarily on power conservation.

Inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay. Many researchers are currently engaged in developing schemes that fulfil these requirements. In this paper, a survey of protocols and algorithms proposed thus far for sensor networks. The aim is to

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

provide a better understanding of the current research issues in this field.

Attempt an investigation into pertaining design constraints and outline the use of certain tools to meet the design objectives. The flexibility, fault tolerance, high sensing constancy, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this spacious range of application areas will make sensor networks an integral part of our lives.

However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, expense, hardware, topology change, circumstances and power consumption. Since these bounds are highly stringent and specific for sensor networks, new wireless ad hoc networking systems are required.

C. Towards Event Source Un-Observability With Minimum Network Traffic In Sensor Networks

Yang.Y,et al (2008) provides a stronger notion: event source un-Observability, which promises that a global rival cannot know whether a real event has ever occurred even if he is capable of collecting and analysing all the messages in the network at all the time. Obviously, event source un-Observability is a desirable and critical security property for event monitoring applications, but regrettably it is also very difficult and expensive to achieve for resource-constrained sensor networks. Sensor networks have been envisioned to be very useful for a broad spectrum of emerging civil and military applications.

However, sensor networks are also confronted with many security threats such as node compromise, routing interruption and false data injection, because normally operate in unattended, harsh or hostile environment. Among all these threats, privacy (especially source anonymity) is of special interest since it cannot be fully addressed by traditional security mechanisms such as encryption and authentication. Consider a simple example of event broadcasting in sensor networks.

When a sensor detects an event, it sends a message including event related information to the base station. If an attacker (the hunter here) can intercept the message, it may know such aware information as whether, when and where a concerned event has happened, e.g., the advent of an endangered animal in a monitoring sensor network.

Moreover, sensors typically have low-cost radio devices that employ standardized wireless communication technologies, which allow an attacker to easily proctor, or eavesdrop in communications between sensors. Consequently, it is also feasible for a single attacker to monitor all the network traffic either by deploying his own sensors that cover the whole deployment area or by employing a powerful site surveillance device with hearing range no less than the network radius.

Despite its importance, so far, sensor source unrecognizable has not received enough attention, and the existing solutions have limitations when directly applied to sensor networks. For example, in phantom routing, the attacker has restricted coverage, comparable to that of sensors. Therefore, only a single source is under the attacker's consideration at a time and the attacker tries to trace back to the source in a hop-by- hop fashion.

When the attacker becomes more powerful, e.g., has a hearing range more than three times that of the sensors, the capture likelihood is as high as 97%. In addition, a large number of anonymity techniques designed for general networks are not appropriate to be used for sensor networks. This is not only because the confidentiality problem is different but also because these techniques are too expensive to be employed. In this paper, aim to provide source unrecognizable for sensor networks under a global observer who may monitor and analyse the traffic over the whole network.

Clearly, if all the traffic in the network is real event messages, it is unlikely to achieve source unrecognizable under such a strong attack model. Therefore, employ network-wide mock messages to achieve global privacy. The basic appreciation is as follows. Every node in the network sends out mock messages with intervals following a certain kind of distribution, e.g., allegiance or probabilistic. When a node spot a real event, it broadcast the real event messages with intervals following the same distribution. As such, neither can an attacker be aware of the occurrence of a real event, nor can he find out the locality of the real event source.

To reduce the extra overhead caused by dummy messages, the message transmission rate should be quite low. In this case, however, the real event description latency could be high, because a source node needs to postpone the transmission of a real event message to the next interval. Therefore, more specifically, make the following contributions in this paper. First, demonstrate that it is difficult to achieve perfect global privacy without sacrificing performance benefit. Hence, to relax the perfect source anonymity requirement and for the first time propose a notion of statistically strong source anonymity for sensor networks.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Second, devise a realization scheme, called Fit Prob Rate (Fitted Probabilistic Rate) scheme, in which the event notification suspension, is significantly reduced while keeping statistically strong source anonymity, through selecting and controlling the probabilistic distribution of message transmission intervals. In this paper, after analysing the source anonymity problem under the global attacker model, identify the fundamental trade-off between performance and privacy.

For the first time, propose the notation of statistically strong source anonymity for sensor networks. Also devise a realization scheme called Fit Prob Rate, which achieves statistically strong source anonymity under such a specific circumstance. Performance evaluations demonstrate that by this scheme, the event report latency is largely reduced and source location privacy could be preserved even if the attacker conducts various statistical tests. In our future work, investigate different real-world attack models.

D. Towards Statistically Strong Source Anonymity For Sensor Networks

Shao.M, et al (2008) [7] proposes a scheme called Fit Prob Rate, which realizes statistically strong source anonymity for sensor networks. Also demonstrate the robustness of our scheme under various statistical tests that might be employed by the attacker to detect real events. Our analysis and replication results show that our scheme, besides providing source unrecognizable can significantly reduce real event reporting latency compared to two baseline schemes. Sensor networks bear a promising future in many important applications such as military observation, and target tracking.

However, sensor networks are also confronted with many security threats such as node compromise, routing interruption and false data injection, because normally operate in unattended, harsh or hostile environment. Among all these threats, privacy is of special interest to us since it cannot be fully addressed by traditional security mechanisms, such as encryption and validation.

When a sensor detects an event, it sends a message including event-related information to the base station. After this, the location of the event source has actually been leaked to the attacker (who may be passively monitoring the network), no matter how resilient the data encryption key is. Furthermore, an attacker may find out more sensitive information: whether, when and where a particular event occurred, e.g., the appearing of an endangered animal in an asset monitoring sensor network. This can help the attacker in capturing the animal, an unsuccessful occurrence.

Preserving event source location privacy, however, is a challenging task in sensor networks, which are characterized by limited resources in energy, reckoning, and communication. Hence, only trivial, energy-efficient privacy conserving mechanisms are affordable in sensor networks. Sensors typically have low-cost radio devices that employ standardized wireless communication technologies. The open architecture of the underlying sensor communication mechanisms enables an attacker to easily monitor or eavesdrop communications between sensors.

Consequently, it is possible for a single attacker to monitor all the network traffic either by deploying his own simple sensors that cover the whole deployment area or by employing a powerful site surveillance device with hearing range no less than the network radius. Despite its importance, source location privacy has not received due attention yet. A large number of anonymity techniques designed for general networks are not appropriate to be used for sensor networks.

This is not only because the privacy problem is different but also because these techniques are too costly to be employed. A few privacy enhancing solutions have been proposed for sensor networks, but assume relatively weak attack models. For example, in phantom routing, an attacker has limited coverage, comparable to that of regular sensors. At any given time, only a single source is under the attacker's consideration and the attacker tries to trace back to the source in a hop-by-hop fashion. When the invader becomes more powerful, e.g., has a hearing range more than three times of the sensors, the scheme performs poorly since the capture likelihood may be raised to as high as 97%.

In this work ,to provide event source un-observer ability under a global attack model, where an attacker can hear and collect all the messages transmitted in the network at all the time. Event source un-Observability promises that an attacker may neither discern the occurrence of a real event, nor find out the location of the real source. This is a stronger notion of privacy than traditional source location privacy that only hides the location of a real source. Under such an attack model, if all the packets in the network are real event packets, unlikely to achieve event source un-Observability, because the transmission of a message, even encrypted, already indicates the occurrence of an event.

Therefore, devise schemes that introduce dummy traffic. A baseline scheme based on such

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

dummy traffic works as follows. Every node in the network sends out messages, either real or bogus, with intervals following a certain kind of distribution (e.g., constant rate or exponential). When a node detects a real event, it delays the transmission of the real event message such that the next inter-message interval follows the same distribution. Although this baseline scheme provides event source un-Observability, it is also prohibitively expensive for sensor networks.

The huge numbers of bogus messages not only consume the constrained energy of sensor nodes for transmissions, but also lead to high channel collision and consequently low delivery ratio of real event messages. Therefore, it is our paramount goal to reduce the traffic while preserving event source un-Observability. To achieve this goal, propose a Proxy-based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS). In PFS, some sensors are selected as proxies to collect and filter dummy messages from surrounding sensors. PFS greatly reduces the communication cost of the system by dropping many dummy messages before reach the base station.

In TFS, proxies are organized into a tree hierarchy. Proxies closer to the base station filter traffic from proxies farther away, thus the message overhead could be further reduced. The message overhead imposed by these schemes is usually dependent on the locations of the proxies. Hence, based on local search heuristics devise a proxy placement algorithm for each scheme to minimize the overall message overhead.

Since real event messages may be delayed at the source due to the need to postpone their transmission, select suitable parameters for the buffers at the proxies to reduce buffering delay while preserving event source un-Observability. Simulation results indicate that our schemes not only find nearly optimal proxy placement efficiently but also yield high delivery ratio and low bandwidth overhead, relative to the baseline scheme. A prototype of our schemes is implemented for Tiny OS-based Mica2 motes, which consumes only about 400 bytes in the RAM space.

The rest of the paper is organized as follows. first describe the problem and build up our model After that, simulation and implementation results. In this paper, solve the optimal proxy placement problem by using local search heuristics and propose a Proxy based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS), which are simple yet efficient event source un-Observability preserving solutions for sensor networks. The two methods work together, so that can maximally reduce the network traffic while increasing the delivery ratio without sacrificing privacy. Performance evaluation demonstrates that our schemes can largely improve the system performance compared with a baseline scheme.

E. De-Correlating Wireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks

Deng.J, et al (2006) described, including hop-by-hop re-encryption of the packet to change its appearance, obligation of a uniform packet sending rate, and deduction of correlation between a packet's receipt time and its forwarding time. More refined countermeasures are described that introduce randomness into the path taken by a packet. Packets may also split into multiple fake paths to further confuse an adversary.

A technique is introduced to create multiple random areas of high communication activity called hot spots to deceive an adversary as to the true location of the base station. The efficiency of these countermeasures against traffic analysis attacks is demonstrated analytically and via simulation using three evaluation criteria: total entropy of the network, total overhead energy paid out, and the ability to frustrate investigative-based search techniques to locate a base station.

In wireless sensor networks, sensor data is typically routed along relatively fixed paths from sensor nodes towards the base station. This produces quite pronounced traffic patterns that reveal the direction towards and hence the location of the base station. the packet traffic volume forwarded by each node in the network with the shortest path routing scheme .The nodes near the base station clearly forward a significantly greater volume of packets than nodes further away from the base station, in the same manner that a river grows wider as it collects more water from its tributaries.

Aggregate nodes that compress the data from multiple child nodes before forwarding upstream towards the base station can mitigate the pronounced increase in traffic volume towards the base station. However, the data traffic still accumulates towards the base station, if the aggregates send their data through multiple hops. An adversary can analyse the traffic patterns revealed to deduce the location of the base station within the WSN's topology. For example, pronounced data traffic patterns in a WSN using SP routing scheme reveal the location of the base station.

- If the contents of a packet being transmitted are in plain text, an adversary can determine which

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

packets are being forwarded towards the base station. This allows the adversary to follow the direction of these packets towards the base station.

- If there is a correlation in time between the instant a node X receives a packet (a neighbour transmits that packet to X) and when node X forwards that packet, an adversary can use this time correlation to identify the same packet as it is relayed hop by hop, and thereby trace the direction towards the base station.
- Given that there is higher communication activity near the base station, an adversary can move closer to the base station by moving towards areas of higher packet traffic.

Since the base station is a central point of failure, once the location of the base station is discovered, an adversary can disable or destroy the base station, thereby rendering ineffective the data-gathering duties of the entire sensor network. A simple defence against plain-text observation is to encrypt each packet. However, if data packets are encrypted, but do not change hop by hop, then an adversary can still follow a given encrypted packet pattern towards its destination, which will often wind up at the base station.

Following the path of encrypted packets can be defeated if each data packet is re-encrypted at each hop, thereby changing the appearance of each packet at each hop, e.g. by employing pair-wise key schemes. Even with hop-by-hop re-encrypted packets, an adversary can still deduce significant information that can reveal the base station's location by monitoring traffic volume, or by looking at time correlations. The act of transmitting itself reveals information to the attacker, regardless of whether packet contents can be inspected. In the case of rate monitoring, the volume of transmissions can be exploited.

In the case of time correlation, an adversary can listen to a transmission and also the next-hop forwarding transmission along a relay path and infer some path relationship between two neighbouring nodes regardless of whether the packet is re-disguised at each hop. Therefore identify two classes of traffic analysis attacks in wireless sensor networks, a rate monitoring attack and a time correlation attack. In a rate monitoring attack, an adversary monitors the packet sending rate of nodes near the adversary, and moves closer to the nodes that have a higher packet sending rate.

In a time correlation attack, an adversary observes the correlation in sending time between a node and its neighbouring node that is assumed to be forwarding the same packet, and infers the path by following the "sound" of each forwarding operation as the packet propagates towards the base station. The paper, focus on developing countermeasures against traffic analysis attacks that seek to locate the base station, particularly against the rate monitoring and time correlation attacks. Given an adversary who is analysing packet transmissions within its range, the overall objective is to significantly delay an adversary from locating a base station. In particular, our goals are:

- An opposition cannot determine a packet destination by inspecting the contents of the packet.
- An opposition cannot find the data flow direction by analysing the time correlation between the packets sent by children nodes and packets sent by their parent nodes.
- An opposition cannot find the data transmission direction by employing statistical analysis of the packet transmission rate of every node within its range.

One way to defend against traffic analysis is to control the packet sending rate of every node in the network in such a way that every node sends packets with the same rate. Describe two methods to control the packet sending rate and packet sending time of each sensor node. These two methods can be used to defend against the rate monitoring and time correlation attacks. However, there are some limitations to these rate control methods. For example, may delay data reports, or introduce too much traffic to the network. To address these limitations, propose four improved techniques in that introduce randomized traffic volumes throughout the sensor network to deceive or misdirect an adversary from discovering the true location of the base station.

First, a multiple parent routing scheme is introduced that allows a sensor node to forward a packet to one of its parents. This makes the patterns less pronounced in terms of routing packets towards the base station. Second, a controlled random walk is introduced into the multi-hop path traversed by a packet through the WSN towards the base station. This distributes packet traffic, thereby rendering less effective rate monitoring attacks. Third, random fake paths are introduced to confuse an adversary from tracking a packet as it moves towards a base station. This mitigates the effectiveness of time correlation attacks. Finally, multiple, random areas of high communication activity are created to deceive an adversary as to the true location of the base station, which further raises the difficulty of rate monitoring attacks.

A natural extension of this approach is to broadcast every packet, which achieves maximum

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

De-correlation at maximum cost. The methods proposed in this paper, e.g. DEFP defined later, achieve close to broadcast's maximal De-correlation, as signified by maximizing the number of search steps by an adversary, at a fraction of the cost, namely about two orders of magnitude less overhead than flooding.

First, all four techniques are distributed in nature. There is no single initialization or coordination point involved to setup these mechanisms. Second, memory and computation requirements in each sensor node are quite low, and can easily be met by modern sensors such as the MICA2 mote. Third, any compromise of one or a small number of sensor nodes by an adversary is easily tolerated.

If an adversary compromises some nodes, the damage it can inflict upon the WSN is limited. Fourth, our techniques don't require a node to delay sending packets. A node can send forward its packet as soon as it is ready. This aids in reducing the time delay introduced by countermeasures against traffic analysis attacks. Finally, the cost of these techniques is moderate and the techniques are applicable to large sensor networks. This is confirmed by simulation results.

The tree-based routing structure of a wireless sensor network is rooted in a base station. The forwarding patterns of WSNs are highly pronounced, revealing the location of the base station through traffic volume and directionality of packet forwarding. An adversary can eavesdrop and employ rate monitoring and time correlation traffic analysis attacks to locate and destroy a base station, thus disabling the entire WSN. This paper proposed a suite of countermeasures aimed at de-correlating network traffic so that the location of a base station is disguised against traffic analysis techniques.

First, three basic defences were proposed that morph a packet's appearance at each hop via re-encryption, impose a uniform sending rate throughout the network, and de-correlate packet sending times at each hop. Next, an improved suite of four more advanced solutions were proposed that overcome limitations of the basic defences. Introduce controlled randomization into the multi-hop path a packet takes from a sensor node to a base station.

Further introduced random fake paths to confuse an adversary from tracking a packet as it moves towards a base station. Finally, create multiple, random hot spots of high communication activity to deceive an adversary as to the true location of the base station. The paper evaluated these techniques analytically and via simulation using three evaluation criteria: total randomness or entropy of the network, total energy consumed as represented by message overhead cost and the ability to prolong a heuristic-based search technique called GSAT to locate a base station.

The simulations showed that our combined suite of advanced randomization techniques, namely multi-parent routing plus controlled random walk plus differential enforced fractal propagation, together achieved de-correlation comparable to the best possible de-correlation represented by broadcast, at a fraction of broadcast's messaging cost.

F. Protecting receiver-location privacy in wireless sensor networks

Jian.Y, et al (2007) proposes a location privacy routing protocol (LPR) that is easy to implement and provides path diversity. Combining with mock packet injection, LPR is able to minimal the traffic direction information that an adversary can retrieve from eavesdropping. By making the orders of both incoming and outgoing traffic at a sensor node regularly distributed, the new defence system makes it very hard for an adversary to perform analysis on locally gathered information and infer the direction to which the receiver locates.

Evaluate our defence system based on three criteria: delivery time, isolation protection strength, and energy cost. The recreation results show that LPR with fake packet injection is capable of providing strong protection for the receiver's location privacy. Sensor network technologies promise drastic enhancement in automatic data collection capabilities through efficient deployment of small sensing devices. A sensor network consists of a large number of resource-constrained sensor nodes.

Each node acts as an information source, collecting data samples from its environment and transporting data to a receiver via a multi-hop network, in which each node performs the routing function. With the accessibility of cheap wireless technologies and micro sensing devices, sensor networks are expected to be widely deployed in the near future. The open nature of wireless communication makes it easy for attackers to eavesdrop or inject data packets in a sensor network.

Furthermore, unlike other wireless networks composed of mobile devices such as laptops and PDA's with human presence, sensor networks are usually adopted in open areas, where unattended sensor nodes lack physical protection. This means attackers will clash with much fewer obstacles when attacking a sensor network. Privacy in sensor networks may be classified into two categories:

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

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 stalled by encryption and authentication.

However, even after strong encryption and authentication mechanisms 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 eavesdropping the network traffic and analysing the traffic patterns. In particular, the locality information about sender's receivers may be derived based on the direction of wireless communications. In this paper, focus on the protection of location privacy for the receiver (or the base station) in sensor networks. It is very important to protect the receiver's location privacy in a sensor network.

First, in many sensor networks, the receiver is the most critical node of the whole network, as the responsibility of the receiver (i.e., the base station) is to collect data from all sensors. Since all sensors forward data to a single node (the receiver), this creates a single point of crash in the network. A sensor network can be delivered useless by taking down its receiver. Second, in some situations, the receiver itself can be highly sensitive. Imagine a sensor network deployed in a battlefield, where the receiver is approved by a soldier.

If the location of the receiver is exposed to adversaries, the soldier will be in great danger. There are several ways that an adversary can trace the location of a receiver. First, an opponent can deduce the location of the receiver by analysing the traffic rate. This traffic-analysis attack is established. The basic idea is that sensors near the receiver forward a greater volume of packets than sensors further away from the receiver. By eavesdropping the packets broadcast at various locations in a sensor network, an adversary is able to compute the traffic densities at these locations, based on which it deduces the situation of or the direction to the receiver.

However, to perform the traffic-rate analysis, an opponent has to stay at each location long enough such that sufficient data can be gathered for computing the traffic rate. This process takes long time as the opponent moves from location to location. Second, an opponent can reach the receiver by following the movement of packets. This packet-tracing attack, where the sender's location privacy, instead of the receiver's, is considered. In this attack, an equipped opponent can tell the location of the immediate transmitter of an overheard packet, and therefore he is able to accomplish hop-by-hop trace towards the original data source. The technique of packet tracing can be used to locate the receiver as well.

Because the packet-tracing attack does not have to gather traffic-rate information, it allows an adversary to move quickly from location to location towards the receiver. The packet-tracing attack may even be able to trace a mobile receiver due to its fast response, although the slow response of the traffic-analysis attack makes it unsuitable for such a task. In this paper, focus on studying the defense measures against the packet-tracing attack. When a traditional single-path routing protocol is used, a sensor network is extremely exposed to the packet-tracing attack, as the routing paths are static and point to the receiver. By Eavesdropping the packet transmission, an opponent is able to move one hop along the shortest path towards the receiver for each packet overheard.

In order to protect the receiver's location privacy, propose a couple of countermeasures against the packet tracing attack. First, propose a new location-privacy routing protocol, called LPR, to provide path diversity. Second, combine this routing protocol with fake packet injection to minimize the information that an adversary can deduce from the overheard packets about the direction towards the receiver. Under such a protection scheme, an opponent can hardly distinguish between real packets and fake packets, or tell which direction is towards the receiver. Defending against the packet-tracing attack is a challenging problem. Cryptography does not help because the adversary deduces information simply by overhearing and following the radio transmissions. In order to remove the directional property in the movement of packets destined for a receiver, a considerable number of obfuscating transmissions have to be made.

To address the overhead problem, design the system in such a way that one can easily tune the trade-off between the protection strength and the overhead introduced in the network. It should also be noted that, if the security of the receiver is of great importance, overhead may be a price that one has to pay even in sensor networks, when better alternatives do not exist. In this paper, design LPR, a location-privacy routing protocol, and combine it with mock packet injection to protect the location privacy of the receiver in a sensor network. Study the packet-tracing attack, in which an adversary traces the location of a receiver by eavesdropping and following the packets transmitted in the sensor network. This attack cannot be effectively responded by the existing approaches.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Our system addresses the affected in two ways. First, LPR randomizes the routing paths. Second, mock packet injection attempts to make both incoming packets and outgoing packets uniformly distributed in all directions at a node. This makes it very hard for an adversary to infer the location of or the direction to the receiver. Moreover, the adjustment between protection strength and energy consumption is made tuneable through two system parameters. Perform extensive simulations to evaluate LPR with false packet injection based on three criteria: delivery time, protection strength, and energy cost. The ravages show that, comparing with other methods, LPR with fake packet injection provides stronger protection for the receiver's location privacy. In the future work, they will extend our study to networks with multiple receivers, and they will also formally analyse the performance of our scheme.

Existing System

The existing solutions can only be used to deal with adversaries who have only a local view of network traffic. A highly motivated opponent can easily eavesdrop on the entire network and defeat all these solutions. For example, the opponent may decide to deploy his own set of sensor nodes to monitor the communication in the target network. However, all these existing methods think that the opponent is a local eavesdropper. If an opponent has the global knowledge of the network traffic, it can easily setback these schemes. For example, the opponent only needs to identify the sensor node that makes the first move during the communication with the base station. Automatically, this sensor node should be close to the location of adversaries' interest.

A. Evaluating the existing security designs in WSNs

Evaluation of existing systems can be done with the help of data security requirements like data validation, availability and validation. Security is not provided cost-effectively by the existing systems due to weak security strengths and is exposed to many different attacks. Security validation tools such as validation and key management. These tools provide various protection mechanisms for sensor network. Routing and localization are ropes sensor network.

B. Limitations of existing key management schemes

From many past years many different pre-distribution schemes have been proposed. Hop-by-hop is one of the procedures which don't provide end-to-end security in a proper manner. It not only involves the end points but also have the intermediate components for data forwarding. Hop-by-hop header carries data which should be examined by each and every node along the packet path. As this procedure involves each node referencing and processing it becomes complex in analysis of networks. Data authentication and confidentiality is very much vulnerable to inside attacks and the multi hopping makes a worse while transmitting the messages.

C. False data filtering and their analysis

This helps in protecting data from validation in WSNs. Data that is not official will be filtered out by the transitional nodes. Location Based Resilient Secrecy (LBRS) is the proposed scheme that identifies the problems and errors in Statistical En-route Filtering (SEF) and Interleaved Hop-by–Hop Authentication (IHA). All these methods are highly exposed to interference attacks and selective forwarding attacks. SEF helps in detecting and dropping the false reports during the forwarding process that contains Message Authentication Codes (MAC) generated by multiple nodes.

D. Drawbacks of Existing System

- The existing approaches assume a weak opponent model where the adversary sees only local network traffic.
- Existing procedures defend the leakage of location information from a limited adversary who can only observe network traffic in a small region.

Proposed System

The performance of the proposed privacy-preserving techniques in terms of energy consumption and latency and compare our methods with the phantom single-path method, a method that is valuable only against local eavesdroppers. For the purpose of simulation, assume that the network application only needs to detect the locations of pandas and always wants to know the most recent locations. Every sensor node drop a new packet if it has already queued a packet that was generated on the same event. In the simulation, Assume that the adversary has deployed a network to monitor the traffic in the target network.

A. Advantages

- The system provides trade-offs between privacy, broadcast cost, and latency.
- This procedures are efficient and effective for source and sink-location privacy in sensor networks.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

- Increased Detection speed and protection for objects and sinks.

B. System architecture

A system architecture or systems architecture is the conceptual model that defines the structure, behaviour, and more views of a system. It serves as a model to describe analyse a system.

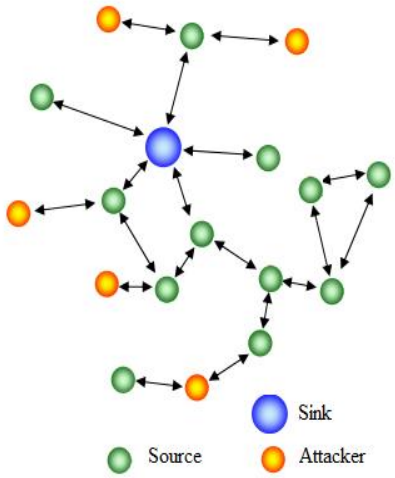


Figure 4.1System Architecture for Sensor Networks.

A. Source-Location

Two techniques to provide location privacy to monitored objects in sensor networks, regular collection and source simulation are proposed. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery potential. The source mock-up method provides practical trade-offs between privacy, broadcast overhead, and latency.

B. Sink-Location

Two privacy-preserving routing techniques for sink-location privacy in sensor networks sink simulation and backbone flooding. The sink mock-up method achieves location privacy by simulating sinks at specified locations, and the backbone flooding method routine location privacy by flooding the event reports in a backbone network that covers the data sinks. Both techniques provide trade-offs in the middle of privacy, communication cost, and latency. This section mainly focuses on protection of passive sinks that only receive data from sensors. This will consider location privacy for sinks that broadcast packets in future work.

C. Attacker

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. In addition, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are divided as active attacks and passive attacks.

Module Description

A. Sensor Network Creation
B. Source-Location Privacy
C. Sink-Location Privacy
D. Performance Analysis.

A. Sensor Network Creation

The event-driven simulator NS2 is used to model the Sensor Network environment in terms of: network model, and traffic model. These two models are described as follows:

- Network model: More than 20 nodes were randomly deployed on a 1000m X 1000m square area, utilizing CSMA/CA without the retransmission mechanism for wireless transmission.
- The maximum transmission range of these nodes depends on whether L1 or L2 transmission is chosen, that is, nodes can reach 100 m when using PL1 and 300 m when using PL2.
- Traffic model: Source nodes in the network use Constant Bit Rate (CBR) traffic type, generating five data packets per second. Each packet is composed of the data consignment and its header with size payload and header respectively. Multicast scenario can be used.

B. Source-Location Privacy

In this Module, two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source mock-up are proposed. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source mock-up method provides practical trade-offs between privacy, broadcast overhead, and latency.

C. Sink-Location Privacy

This module presents two privacy-preserving routing techniques for sink-location privacy in sensor networks, sink simulation and backbone flooding.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The sink mock-up method achieves location privacy by simulating sinks at specified localities and the backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks. Both procedures provide trade-offs between privacy, communication cost, and latency. This section mainly focuses on protection of passive sinks that only receive data from sensors. This will consider location privacy for sinks that broadcast packets in future work.

D. Performance Analysis

In this section, the results obtained from the simulation are analysed. The following three aspects:

- End-to End Delay
- Routing Overhead
- Packets generated are analysed.

References

[1] *M. King, B. Zhu, and S. Tang, "Optimal path planning," Mobile Robots, vol. 8, no. 2, pp. 520-531, March 2001.*

[2] *H. Simpson, Dumb Robots, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.*

[3] *M. King and B. Zhu, "Gaming strategies," in Path Planning to the West, vol. II, S. Tang and M. King, Eds. Xian: Jiaoda Press, 1998, pp. 158-176.*

[4] *B. Simpson, et al, "Title of paper goes here if known," unpublished.*

[5] *J.-G. Lu, "Title of paper with only the first word capitalized," J. Name Stand. Abbrev., in press.*

[6] *Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Translated J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digest 9th Annual Conf. Magnetics Japan, p. 301, 1982].*