AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Protecting Location Privacy on Sensor Networks Against Global Eavesdropper

[1]R.G. Suresh Kumar, [2]T. Nalini , [3]V. Susmitha, [4]J. Nivedhidha

[1]*Research Scholar, Vels University, Chennai, India*
[2]*Professor, Bharath University, Chennai, India.*
[3,4]*M. Tech Student, Rajiv Gandhi College of Engineering &Technology, Puducherry, India.*

Address For Correspondence:
R.G. Suresh Kumar, Research Scholar, Vels University, Chennai, India
E-mail: aargeek@gmail.com

ARTICLE INFO

Article history:
Received 26 April 2016
Accepted 21 July 2016
Published 30 July 2016

Keywords:
Network Traffic, Source Simulation, Sink Simulation, Backbone flooding.

ABSTRACT

In wireless sensor network (WSN) which contains of more number of small multi-operational ,resource-constraint sensors and are self- structured as an ad-hoc network to track the real world. A wireless sensor network is a set of specialized transducers with communications infrastructure used for monitoring and recording conditions at various locations. Commonly monitored parameters in wireless sensor network are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.Sensor networks are widely used in applications where it is not feasible to set up wired networks.A sensor network consists of multiple tracking stations called sensor nodes, which is small, lightweight and portable. Each sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery source. Some of the examples are wildlife habitat tracking, security and military inspection and for target monitoring. The existing solutions are focused to deal with adversaries it has only a confined view of network traffic.An adversary can easily spy the whole network and beat all these solutions For example, an adversary may determine to build his own set of sensor nodes to view the communication in the whole network. We then shape the location privacy issues under the powerful adversary model and then display the details communication overhead which plays an important role for achieving a given level of privacy. We also propose two techniques which halt the leakage of location information : which covers periodic collection and source simulation.In this paper we also propose two methods for providing protection over data sink : which includes sink simulation and backbone flooding. Periodic collection which contributes to high level of location secrecy, where source simulation provides balance between privacy , communication overhead cost and latency. By using analysis and simulation process, we denote that proposed techniques are efficient and effective in preserving location information from the intruder.

INTRODUCTION

In wireless distributed system, which disperse autonomous sensors to track the physical or environmental conditions such as temperature, sound, pressure etc. and to collectively send their data through to central location. More advance networks are of two way communication and also permit control over sensor activity. Growth of wireless sensor network was encouraged by military applications whereas in battlefield supervision,

To Cite This Article: R.G. Suresh Kumar, T. Nalini, V. Susmitha, J. Nivedhidha., Protecting Location Privacy on Sensor Networks Against Global Eavesdropper. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 76-81, 2016*

and nowadays these kind of networks are used in many industrial and consumer application which include industrial operation monitoring and control, machine health monitoring and as follows (Akyildiz, W *et al*.., 2002). The WSN is constructed by nodes from a small number to several hundred or even thousand where each node to one or more number of sensors. Each sensor network node consists of several parts: a radio transceiver has an in-build antenna or link through an external antenna , a microcontroller, and also includes electronic circuit for interacting with its sensor and power source or embedded form of energy harvesting. A sensor node changes in size from a shoebox down to the size of a grain of dust, all above functioning "motes" of genuine microscopic dimensions are yet to be constructed. The cost of sensor node is changeable from a few to hundreds of dollars, depending on the complexity of individual sensor nodes. Size and cost constraints on sensor nodes which produce solution in corresponding constraints on resources such as energy, memory, computational speed and communication bandwidth. The topology of WSN may vary from a star network to further multi-hop wireless mesh network.

II Development And Its Standards:

In this development and standards which includes a complete description of communication network standard, topologies and components (Akyildiz, W *et al*., 2002).

(i) Ethernet The Ethernet has been evolved in the mid 1970's by Xerox, DEC, and Intel and was normalized in 1979. The Institute of Electrical and Electronics Engineering released the formal Ethernet standard IEEE 802.3 in the year 1983. The Fast Ethernet operates at ten times faster than the speed of regular Ethernet, and was executively adopted in 1995. It establishes new features such as full duplex operation and auto negotiation. Both of these standards use IEEE 802.3 variable length frames between 64 and 1514- byte packets.

(*ii*) *Token Ring* IBM introduced the 4Mbit/s token ring network in 1984.The system supports high quality and robust. The IEEE standardized the token ring by using IEEE 802.5 specification. The Fiber Distributed Data Interface FDDI mention a 100Mbit/s token-passing, dual ring LAN that uses fiber optic cable. It was stabilized by the American National Standard Institute (ANSI) in the mid-1980, and its current capabilities speed exceed far away from Ethernet and IEEE 802.5 standards.

(*iii*) *Gigabit Ethernet* The Gigabit Ether*net al*liance introduced in the year 1996, and Gigabit Ethernet standards came to contract in 1999, which specifies a physical layer using a mixture of both original Ethernet and fibre optic cable cable technologies which evolved from FDDI.

(*iv*) *Client-Server* Networks became familiar in the late 1980's with the replacement of large mainframe computers by personal computer networks. Application programs used in distributed computing environments are essentially divided into two parts: the client as front end and the server as back end. The user's personal computer is the front end and powerful interface machine interface with the networks.

(*v*) *Peer-to-Peer networking* These networking architectures have all computers with equivalent capabilities and responsibilities. In this network no server and computers are connected with each other. They actually make use of bus topology to share files, printers, Internet and also for sharing other resources etc.

(*vi*) *Peer-to-peer computing* There is an next evolutionary step over p2p networking. The computing tasks are divided between many no of computers and the outcome are assembled for further consumption. P2P computing has sparked a revolution over Internet age and has obtained success in a very short time.

III Communication Networks:

To understand and to implement sensor networks, however several basic concepts are to be discussed here The primary issue in communication network is the transmission of messages to achieve a prescribed message throughput and quality of service (Qos). Qos can be specified in terms of message delay, error bit rates, packet loss, transmission cost, power transmission etc. Basically a communication network is composed of nodes, which has computing power and can transmit or receive messages over communication links, wired or wireless (Bamba, B., *et al*., 2008). A single network consists of several interconnected subnets of different topologies. Networks are classified into Local area network (LAN) and wireless area network(WAN).

(i) Fully connected network They suffer from problems of NP-complexity. It also has some additional nodes and the number of links increases exponentially. Therefore for large networks, the routing problem is computationallyintractable with the available amount of computing power.

(ii) Mesh Network Generally distributed networks which allows communications with the nearest neighbours. In these networks nodes are actually identical in nature. Mesh nets can be one of the model for large-scale wireless sensor networks distributed across geographic region, eg. Personnel or vehicle security surveillance systems.An advantage of mesh nets is although all nodes may be identical and have the same computing and transmission capabilities such nodes can be designated as group leaders and has additional functions. All nodes in star topology are connected to a single hub which requires message handling, routing, and decision making abilities compare to the other nodes. In the ring topology, messages generally travel around the ring in a single direction. However if the ring is cut all communication get lost. The self-healing ring

network(SHR) has two rings and they are more fault tolerant.whereas in bus topology each node checks the destination address in the message header and the process the message addressed to it.

(iii) 802.11 Wireless Local area network IEEE ratified the IEEE 802.11 specification in 1997 as a standard for WLAN. Today versions of 802.11 which provide support for transmission upto 11Mbit/s. WiFi is one of the known as fast networking for connecting PCs, printers, and other devices in a local environment. For example The home where users purchase and install a Wi-Fi router which provides supports for connecting various devices like laptops, personal computer and mobile phones etc.

(iv) Bluetooth It was founded in 1998 and formalized by IEEE as Wireless personal area network (WPAN) specification IEEE 802.15. Bluetooth supports short range radio frequency technology which aims at communication with other electronic devices and allows for data synchronization which is transparent to the users. Supporting devices include PCs, laptops, printers, joysticks, keyboards, mice, cell phones, PDAs, and consumer products and discovery protocols which allow new devices to be hooked up easily with the network. Bluetooth uses unlicensed 2.4GHz band to transmit data upto 1Mbit/s and it has a nominal range of 10m that has been extended to 100m. A master station can service upto 7 simultaneous slave links.

(v) Home RF It was introduced in 1998 and has bluetooth goals to attain WPAN. Its major goal is to share data/voice transmission. It interfaces with the internet and public switched telephone network. It uses 2.4 GHz and has range of 50m.A maximum of 127 nodes can be included in a single network. IrDA is a WPAN technology that has a narrow transmission beam which is suitable for aiming at selective reception of signals.

IV Applications Of Wireless Sensor Networks:

(i) Area Monitoring In Area Monitoring the WSN is implemented over a particular region whereas some circumstances need to be monitored For example In military they make use of sensors to detect enemy intrusion.

(ii) Heath Care Monitoring WSN provide support for medical applications they are of two types : wearable and implanted. Wearable devices are used on the top of body surface of human and whereas implanted medical devices are inserted into the human body. It also supports many other applications for example body position measurement and overall monitoring of ill patients in hospitals and at homes.

(iii) Air Pollution Monitoring WSN has been implemented across various cities to detect the concentration of dangerous gases for the citizens. It has advantages of ad hoc wireless links rather than wired installations.

(iv) Forest Fire Detection A network of sensor nodes are installed in the forest to detect fire .Actually the nodes are build with sensors to measure temperature, humidity and gases which are caused by fire in the tree and vegetation. The advance detection is somewhat difficult for the successful action of the firefighters. They make use of fire brigates to detect the time of fire started and spread through the forest.

(*v) Landslide Detection* This system makes use of wireless sensor network to monitor the slight movements of the soil and changes occurs in various parameters which may before or after landslide

(*vi) Water Quality Monitoring* It involves analyzing water properties in dams, rivers, lakes and oceans as well as underground water reserves. Many wireless distributed sensors allows for the creation of more accurate map of the water status and grants for the stable deployment for monitoring stations of different locations of various access which avoids the need for manual data retrieval.

(*vii) Natural Disaster prevention* Wireless sensor networks which act to prevent the effect of natural disasters like floods. Wireless nodes are successfully been implemented in rivers where water level changes are to be monitored in real time.

(viii) Machine Health Monitoring Wireless sensor networks are been developed for machinery condition-based maintainence they also offer cost savings and enables new functionality. Previously inaccessible locations, rotating machinery, hazardous or restricted areas and mobile assests can be attained with wireless sensors.

(ix) Data Logging Wireless sensor networks are used for the collecting data for monitoring the environmental conditions. It has been used to monitor the temperature in a fridge .The statistical information can be used to show how systems are working. The advantage of WSN over regular logger is live and data feed is possible.

(x) Water/ Waste water Monitoring It has been used to monitor the quality and level of water which also includes many activities such as for checking the quality of underground surface water for protecting the country's water infrastructure for the sake of both human and animals.

V Characteristics:

The main characteristics of a WSN include:

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes

- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use.

VI System Overview:

A.Existing System:

The existing system are used to deal with adversaries and they have only a local view if network traffic. A high incentive adversary can easily intrude the whole network and conquest all these solutions. For example the adversary may take his own actions to implement his own set off sensor nodes to monitor the communication in the target network. If an adversary has global knowledge over the network traffic it can easily vanquish these schemes.The adversary need to identify the sensor node that makes its primary move during base station communication[7]. Intuitively this sensor node should close to the location of adversaries.

B. Issues In The System:

The existing system can be used to deal with the adversaries control over the network traffic. An adversary can easily eavesdrop the whole network and conquer all solutions (BlueRadios, 2006). For example, an intruder may implement his own set of sensor nodes to monitor the communication in the targeted network. This is particularly true in industrial spying context where the incentives gain much information from observing the traffic in the targeted network. In the global view of the network traffic, an intruder can easily infer the locations of viewed objects. For example the sensor node that initiates the communication with the base station which is close to the object location (Ghinita, G., *et al*., 2008).

- Contextual information remain exposed.
- Attacks can undermine network applications.
- No location privacy to data sinks in networks.
- Energy consumption is very large.

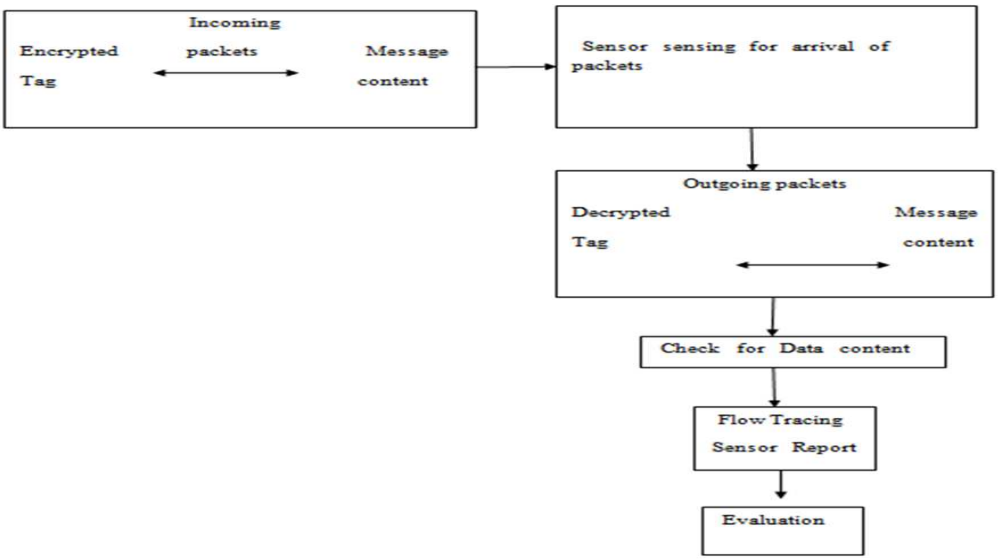

Fig. 1: System Architecture

C. Solutions:

Specifically, it is able to locate every sensor node in the target network and eavesdrop every packet this node delivery (Bollobas, B., *et al*., 2004). Two techniques provide location privacy to monitor objects(source-location privacy):

1.Periodic collection

2.Source simulation .

The other two provide location privacy to data sinks(sink location privacy):

1.Sink simulation

2.Backbone flooding.

D. Proposed System:

Proposed system performance are analyzed using privacy preserving techniques by energy consumption and latency and then we compared our methods with the plantom single-path method, which was effective against local adversary. For simulation purpose we assume that network applications need to detect the pandas locality and always keeps track of the current locations.We have each sensor node to drop a new packet which was already queued a packet generated based on the event .In simulation process we assume the adversary has implemented a network to detect the traffic in the targeted network (Deng, J., *et al*., 2004).

- Provide security for both the monitored objects and data sinks.
- Contextual information will remain unexposed in any big traffic.
- Provides trade offs between privacy, communication cost and latency.

VII Implementation Details:

i) Attackers Module:

Appearance of an endangered animal in a monitored area is survived by wireless sensor, at the each time inside and outside sensors are used to find out the attackers locations and its timing.This information is then passed to the server (http://www.slideshare.net/paterneson/dsr-aodv performance). After verifying the commander and hunter participation in this wireless network. Our motive is to capture the attackers before attempting to hack the network.

ii) Privacy Preserving Routing Techniques:

It consists of two techniques for preserving routing in sensor networks they are periodic collection method and source simulation method. The periodic collection method achieves the optimal location privacy and can be applicable only for the applications which collect data at low rate and do not have harse requirement on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost and latency.It can only be applied for real time applications. In this paper we consider communications between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appears in an random manner to the world wide eavesdropper (Deng, J., *et al*., 2009). This protects the adversary from corresponding different data packets to trace the real object.

iii) Adversary Module:

In this kind of wireless sensor networks we envisioned and expected the well-funded attackers whose objective is to learn sensitive location based information. These information include the events location is detected by target sensor network such as the presence of panda. The Panda- Hunter application was introduced to describe and motivate our techniques. In this application , a sensor network has been implemented to track the endangered giant pandas in the bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by sensors present in the network (http://www.cs.bu.edu/groups). In any case it is feasible to monitor the communication patterns and event location in a sensor network via global eavesdropping. An attacker poses a threat to location privacy in these type of networks and focus our attention to this kind of attacker inside the network.

iv) Privacy Evaluation Module:

In this model, we standardize the location secrecy issues under the global attacker model.The adversary implements an attacking network to monitor the sensor activities in the targeted network. We assume an powerful adversary who has the ability to eavesdrop the every sensor node in the network. Every sensor node i in the target network at time t.In this paper we only consider the attacker to monitor the wireless channel and the contents of any data packets which appear in random manner to the attacker.

v) Security Analysis:

Generally the number of packets are hidden in the secure routing scheme through link-to- link encryption. In this way the attacker cannot find the number of packet for their further processing[9]. Secure routing paths are required to establish at the beginning of each session during the packet transmission, secure routing paths are not required to change for each time.

VIII Simulations:

Most of the commercial simulators are GUI driven, while some network simulators require input scripts or commands (network parameters) (http://www.firstpost.com). The network parameters describe the state of the network (node placement, existing links) and the events (data transmissions, link failures, etc). An important output of simulations are the trace files. Trace files can document every event that occurred in the simulation

and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week, or month, in order to reflect average, worst-case, and best-case conditions. Network simulators can also provide other tools to facilitate visual analysis of trends and potential trouble spots . Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events – such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.Some network simulation problems, notably those relying on queuing theory, are well suited to Markov chain simulations, in which no list of future events is maintained and the simulation consists of transiting between different system "states" in a memory less fashion. Markov chain simulation is typically faster but less accurate and flexible than detailed discrete event simulation. Some simulations are cyclic based simulations and these are faster as compared to event based simulations (htttp://www.slideshare.net). Simulation of networks can be a difficult task. For example, if congestion is high, then estimation of the average occupancy is challenging because of high variance. To estimate the likelihood of a buffer overflow in a network, the time required for an accurate answer can be extremely large. Specialized techniques such as "control variates" and "importance sampling" have been developed to speed simulation.

Conclusion:

Existing work is on location privacy which deals with sensor networks and assumed that attacker has only local eavesdropping capability. Assumption made is unrealistic under a highly motivated attacker. In this paper, we standardize the location secrecy issues under global eavesdropper and showed the minimum average communication overhead which was needed for achieving a given level of privacy. We also presented two techniques which provides privacy against a global eavesdropper. Analysis and simulation techniques studies showed how effectively and efficiently protect location privacy in sensor networks. In particular in this paper we assume that global eaves dropper will not compromise sensor nodes. The eavesdropper is able to perform traffic analysis without looking at the packet content. In practice the global eavesdropper can be able to compromise a few sensor nodes in the field and perform traffic analysis with additional knowledge from insiders.This presents an interesting challenges on both approaches

Future Enchancement:

In addition, We are also interested in the implementation of our methods on real sensor platforms and experimental results from real world sensor application

REFERENCES

Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, 2002. Wireless sensor networks: A survey. Computer Networks, 38(4): 393-422.

Bamba, B., L. Liu, P. Pesti and T. Wang, 2008. Supporting anonymous location queries in mobile environments with Privacy- Grid.In Proc. Intl. Conference on World-Wide Web (WWW*)*.

BlueRadios, 2006. Inc. Order and price info. http://www.blueradios. com/orderinfo.htm. Accessed in.

Bollobas, B., D. Gamarnik, O. Riordan and B. Sudakov, 2004. On the value of a random minimum weight Steiner tree. Combinatorica, 24(2): 187-207.

Ghinita, G., P. Kalnis, A. Khoshgozaran, C. Shahabi and K.L. Tan, 2008. Private queries in location based services: anonymizers are not necessary. In *Proc. ACM Intl. Conf. on Management ofData (SIGMOD).*

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. In *Proc. IEEE Symposium onSecurity and Privacy (S&P)*, pp: 197-213.

Deng, J., R. Han and S. Mishra, 2003. Enhancing base station security in wireless sensor networks. Technical Report CU-CS-951-03, Dept. of Computer Science, University of Colorado.

Deng, J., R. Han and S. Mishra, 2004. Intrusion tolerance and antitraffic analysis strategies for wireless sensor networks.In *Proc.Intl. Conf. on Dependable Systems and Networks (DSN).*

Deng, J., R. Han and S. Mishra, 2006. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. ElsevierPervasive and Mobile Computing Journal, 2: 159-186.

http://robotarm4.hubpages.com/hub/Install-NS2-in-ubuntu

http://www.firstpost.com/topic/product/ubuntu-how-to-run-ns2-program-on-ubuntu

htttp://www.slideshare.net/xeon40/attacks-on-mobile-ad-hoc-networks

http://www.slideshare.net/paterneson/dsr-aodv performance

http://www.cs.bu.edu/groups/itm/SATS/simulation.html