AN ENHANCING SECURITY FOR MOBILE SINKS BY PROVIDING LOCATION PRIVACY IN WSN

N.Bhavya[1], PL.Rajarajeswari[2], N.K.Karthikeyan[3]

[1]*PG Scholar, CSE, Sri Krishna College of Technology, Tamilnadu, India*
[2]*Assistant Professor, CSE, Sri Krishna College of Technology, Tamilnadu, India*
[3]*Associate Professor, CSE, Sri Krishna College Of Engineering & Technology, Tamilnadu, India*

Abstract

A huge collection of sensed data is transacted in Wireless Sensor Networks. This sensed data are reported to the sink. These sinks can be predefined data rendezvous points via multi hop communications. Basically WSNs (Wireless Sensor Networks) plays a key role in applications such as military, remote sensing, etc. Attackers may locate the sink easily by reading the destination field in the packet header or predicting the arrival of the sinks. Data are forwarded along random paths and stored at intermediate points. A random data collection scheme was used to protect the location privacy of mobile sinks in wireless sensor networks. By the sink will move randomly to collect data from local nodes. The goal of the system is to prevent the attackers from predicting their locations and movement of the sink is private. We also protect the sink by data collection at random time intervals and unequal visiting probability.

Keywords: *Wireless sensor networks, Application layer, Data collection, Protocols.*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks are used to report sensed data to sink at different location. Sensors are typically deployed in a high density manner and in large in quantities. The location information of the sinks, sensing devices, and objects should be confidential. Source location privacy concerns about protecting the location information on the data sources. The destination nodes or the sinks whose locations are discovered by the adversary may become the target attacks. The random data collection scheme is used to keep the location and movement of the sink is private. The sensors have to know the location of sinks or rendezvous points. Multi-hop networking reduces the long range transmission since signal path lost in tan inverse exponent with range of particular distance. Each node in the sensor network can act as a recidivist thereby reducing the link coverage required and in turn the transmission power. With the promising sense and wireless technologies also sensor networks have been widely deployed in a broad spectrum of civil and military applications.

The way that data and questions are forwarded between the base station and the location where the target phenomena are observed is authoritative aspect and a basic feature of WSN. A simple access to accomplishing this task is for each sensor node to transfer data directly with the base station. A single hop based approach is costly as nodes that are farther away from the base station may deplete their energy reserves quickly, thereby severely limiting the lifetime of the network. In a multi hop WSN, intermediate nodes must attends in forwarding data packets between the source and the destination. Determining which set of intermediate nodes is to be selected to form a data forwarding path between the source and destination is the principle task of the routing algorithm.

2. RELATED WORKS

There are unusual activities in every field, computers being no exception. People like to store private information on computers. If a criminal was able to slip onto your network, they would be able to access any unguarded computer, and retrieve information off of it once they have access. Make sure you keep at least one password on every computer you own, multiple different ones if it allows it. Network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modifications or denial of the computer and network - accessible resources. The internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. Sensor nodes have wireless communication capabilities and some logic for signal processing, topology management and transmission handling. For WSNs often require in network processing, even while the data are being routed. Security is the most important need of every organization. Especially effective Internet Security has become an essential need for every small, medium or large enterprises using information technology and other internet based services to perform their work easily and effectively. The organization's dependency over Internet has increased the need for internet security

implementation and network monitoring inside the organization.

We consider a wireless sensor network consisting of a number of sensors deployed in an area, together with one or more mobile sink(s). Each sensor has a limited transmission range for wireless communication which allows it to exchange messages directly with its neighboring nodes .Sensors collect data and store them temporarily in the network. The sinks will walk randomly in the field and broadcast occasionally to some local sensors to collect sensing data. Since sensors have limited storage, communication range and computation power, they cannot afford the relatively expensive asymmetric cryptography. Instead, they use symmetric cryptographic primitives to provide data confidentially, authentication, integrity, and freshness of the message. We assume that each sensor shares a unique symmetric key Ki with the sink. Note that multiple sinks can share the same symmetric key Ki with i. We model the step-wise movement of the sink by a Markov chain with a state vector indicating the probabilities of the sink being at different locations. The transition probability matrix between these locations is built based on the step-wise movement of the sink. We calculate p as the stationary distribution of the state vector, which indicates the average probabilities of the sink at different locations in a long run. We show that the sink has equal probability to visit any of the grid points, given that the sink is moving with random steps in the grid.

3. NETWORK MODELS

3.1 Data Storage Approach

For data storage strategy, we compare our approach with fully distributed data storage and uniformly distributed data storage. In fully distributed data storage, the data will be flooded to all the nodes in the network. So that it is easier for the attacker to predict the location of the sink. We show the communication overhead and the success probability for an attacker to predict the location of the sinks. We compare our random path strategy with the classic rendezvous approach for mobile sinks. In the rendezvous approach, the sink visits only a set of rendezvous points, to collect sensing data. Although this approach can shorten the path of a mobile sink, it is vulnerable to the movement prediction attack

3.2 Attacks

We analyze the protection strength of our scheme against different kind of attacks that can capture or trace the location of the sink.

3.2.1 Detaining the Packets

In our random data collection scheme, the sensors only report data to the sink when the sink arrives at the Neighborhood. The communications are limited to the sink's local neighbors. Also, the data are forwarded along random paths for temporary storage. Routing from the sensors to the sink is not required, so the attackers cannot read the sink by reading the destination field of the packets. The attack performed is simply a random guess with a successful probability of 1/Ns, where Ns is the number of sensors in the network.

3.2.2 Observing Network Traffic

The sink moves around to collect data only from its local neighbors in our scheme. The sensors report data to the sink only when it approaches them. Since this mechanism does not require multi-hop routing to the sink, passive attackers will not be able to capture the sink by observing the network traffic. Again, the successful probability of the attack by a random guess is 1/Ns.

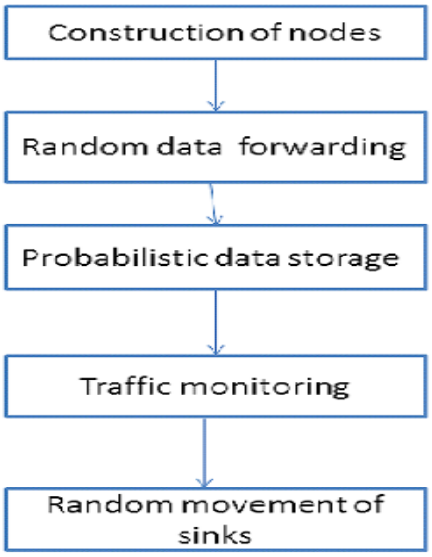
3.2.3 Predicting Movement of the Sink

The sink can move in one out of four directions randomly to collect data in our scheme. It broadcasts to its local neighbors Nb every time interval a. An insider attacker may capture the sink's location when the sink comes nearby to collect data. Since the data are randomly stored and the sink may visit any random locations, an attacker can only stay at a random place and listen to the arrival of the nodes. Suppose that the sink will move for steps before another broadcast.

Sensors are typically deployed in a high-density manner and in large quantities; A WSN consists of densely distributed nodes that support sensing, signal processing, embedded computing and connectivity; Wireless Networks typically transmit information to collecting stations.

4. OUR CONTRIBUTION

The proposed system is that it prevents the attackers from obtaining the destination of the packet even though they are overhearing the messages at the intermediate nodes. The data is collected successfully if the sink is visits any of the nodes caching the data given that the data is still in the cache. The sink broadcasts only to a limited number of neighboring nodes , the chance for an attacker to know the sinks current location is slow. It will also be quite impossible for the attacker to trust or predict the movement of the mobile sinks to do its random movement. Finally we proposed a random data collection scheme to protect the location privacy of mobile sinks in WSNs. Our scheme avoids the location of the sinks to be tracked so as to protect the sinks from becoming the target of attacks. Sensor reports its measurement to the sink, it encrypts the message with its symmetric key and forwards the data along a random path. Node generates a data it stores a copy locally . Then, it forwards the data to some random nodes for storage and for reporting the data to the sink



(a)Flow diagram

4.1 Random Data Forwarding

The process is repeated along nodes on a random path Even the location of the sink is not known ,the data source forwards the packet randomly to any of its neighbors. The next hop receives the packet, it again forwards the packet to one of its neighbors randomly and increments the hop count. However, it will not forward the packet back to the previous hop. The hop count field h in the header of the packet is initialized to zero by the source node. It indicates the number of hops that the packet has travelled. This extension can help distributing the data more evenly in the network. The data is collected successfully if the sink visits any of the nodes caching the data, given that the data is still in the cache.

4.2 Probabilistic Data Storage

When an intermediate node receives a packet, it will store the data in its buffer with a probability ps. Each sensor has a FIFO queue to hold all the data in the buffer. The buffer of each sensor has a limited size, The data will be stored one after another until the sink drops by and clears up the buffer. If the buffer is full, the node will remove the oldest data to free the space for the newly arrived data. It always removes the data at the head of the queue. When a data is brought into the buffer, it will insert the new data at the tail of the queue.Since the packet does not include any destination field, an adversary A1 cannot obtain the location of the receiver even though it can capture an intermediate node and read the packet. Another adversary A2, which is equipped with an antenna to overhear the network traffic, he cannot predict the sink location by traffic monitoring as the packet travels along a random path with no specific destination. The flow of the packet in our scheme is totally independent of the location of the sink.

4.3 Random Movement of Sinks in Data Collection

The mobile sink moves around the network to collect data from the sensors. To avoid being attacked and tracked, it changes its direction randomly and only requests data from its local neighbors occasionally. The mobile sink broadcasts to request sensing data from its neighboring nodes. In each broadcast, the sink will collect all the data in the buffer of its neighboring nodes. This allows the sink to explore the sensing field at any chosen location or direction not limited to its locality. The sink can move from one waypoint to another along a straight line or with zigzag movement. After arriving at the destination, it chooses a new waypoint and moves to it as a new destination.

5. CALCULATION

To calculate the average probability pa of a sensor to get a new piece of data in each time slot. A node can get new data either by generating itself or receiving a copy of data generated by its surrounding neighbors (within L hops). We consider that each node has equal probability ps to generated new piece of data in one time slot. For each source nodes, its surrounding nodes within L hops will have a decreasing probability to receive a copy of that data. Let pe, ps, pw, and pn be the probability of forwarding the data to the next hop following the four directions (east, south, west, and north respectively). If the data is generated by node s at coordinates (x,y), then the probability of the neighboring nodes to receive the data is calculated as below. Note that the results in brackets are calculated with pe, ps, pw and pn all equal to 0.25.

In the first step:

$$P(x+1,y)=pe(=0.25)$$
$$P(x,y-1) =ps\ (=0.25)$$
$$P(x-1,y) =pw(=0.25)$$
$$P(x,y-1) =pn(=0.25)$$

In the second step:

$$P(x+1,y+1)=pepn+pnpe(=0.125)$$
$$P(x,y-2)=psps(=0.0625)$$

6. IMPLEMENTATION

The random data collection scheme which protects the location privacy of mobile sinks in WSNs. In our scheme the sensors will forward the data along random paths and the intermediate nodes will store the data probabilistically. The mobile sink will walk randomly in the network and collect data from the local sensors.

6.1 Construction of Nodes

The random data forwarding consists various nodes. Then it forwards the data to some random nodes for storage and for reporting the data to the sink. At the beginning of the simulation, the delivery rate is low because the data have just been generated and the sink has not visited and collected most of them yet Since the location of the sink is not known, the data source forwards the packet randomly to any of its neighbors. The process is repeated along nodes on a random path and as shown in Fig 5.1

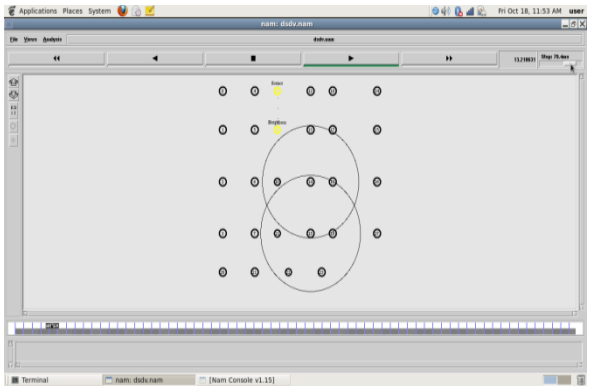


Fig 5.1 Construction of nodes

6.2 Random Paths

In the random paths are described and it forwards the packets one of its neighbors randomly and increments the hop count. It indicates the number of hops that the packet has travelled and as shown in Fig 5.2

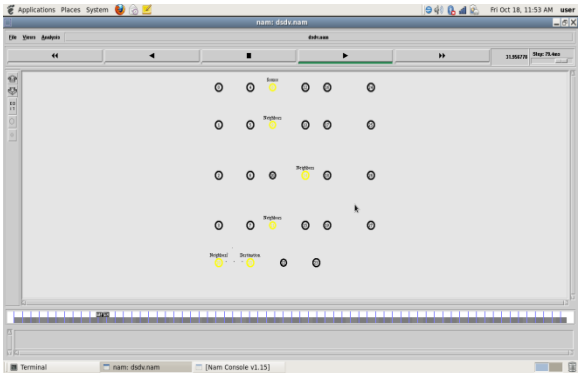


Fig 5.2 Random paths

6.3 Data Caching Model

Each sensor has a FIFO queue to hold all the data in buffer. If the buffer is full, the node will remove the oldest data to free the space for the newly arrived data and as shown in Fig 5.3

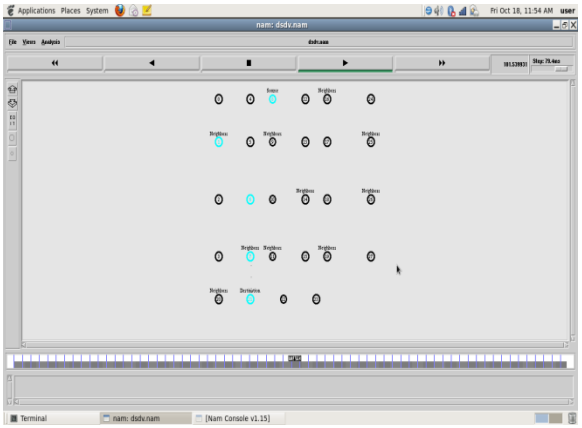


Fig 5.3 Data caching model

6.4 Probabilistic Data Storage Model

The probabilistic data storage explains the intermediate nodes store a copy of the data probabilistically. The data will be stored one after another until the sink cleans the buffer. The packet keeps travelling until the path length is reached. And it is shown in Fig 5.4

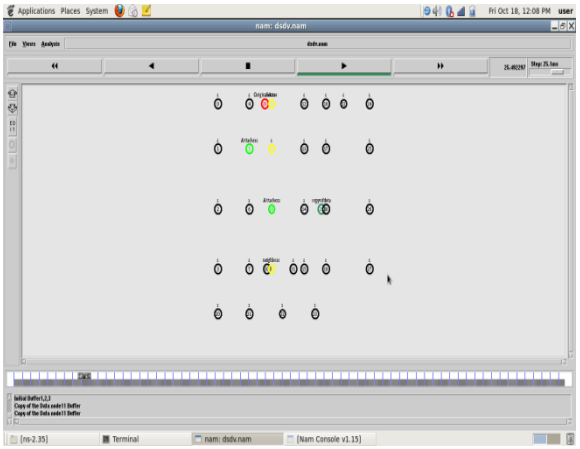


Fig 5.4 Data storage model

The flow of the packet in our scheme is totally independent of the location of the sink.

6.5 Random Movement of Sinks in Data Collection

In the random movement of sinks in data collection explains the mobile sinks move around the network to collect data from the sensors. To avoid being attacked and tracked, it changes its direction randomly and only requests data from its local neighbors occasionally.

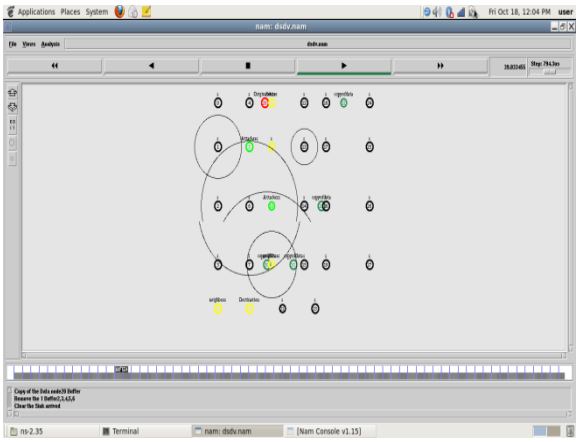
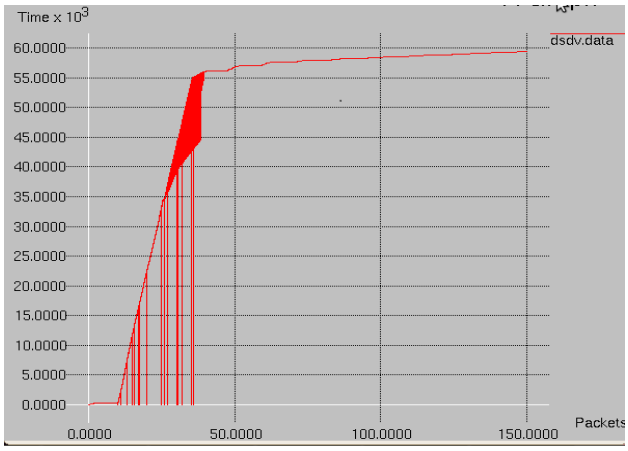
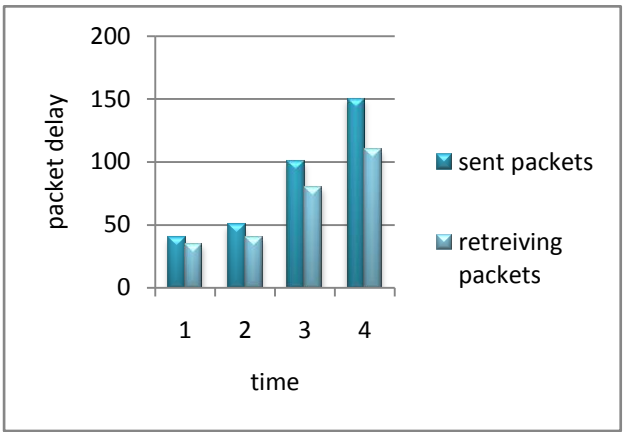


Fig 5.5 Random movement of sinks in data collection

Graph as following,
Consider a number of sensor nodes as shown in the graph. X denotes the time and Y graph indicates the packet delay. Suceessful delivery probabilty varying in buffer size.And over all the protection strength is much higher than the traditional scheme.



In the bar chart Represents number of data and receiving packets in the sink.We also calculate the time taken for the attacker to meet the sink if he waits at the same location. Therefore, the attacker in RP can locate and wait for the sink at a rendezvous point in a much shorter and expected time.The packet delay is the time taken for the data to be collected by the sink.It is measured on unit of seconds and only for the packets that are collected by sink successfully.



7. CONCLUSIONS

In this project, to avoid the location of the sinks to be passed over, thus as to protect the sinks from becoming target attacks. Compare with classic techniques for data forwarding, data storage and sink movements in terms of location privacy, delay and message overhead. We have also evaluated our proposed random data collection scheme by extensive simulations various different parameters the sensing data are stored at some random nodes in the network with the sinks moving around randomly and collecting data from local neighbors. Data collection scheme at random time intervals and unequal visiting probability, to further protect the network from advanced attackers. Finally the protective strength of sink is much greater than the traditional random scheme. Our scheme satisfies the strong probability and increase the path length.

FUTURE ENHANCEMENTS

The future scope is to extend the security for a random collection of particular equal visiting probability. For this method, the energy should be lost in the dummy packet injection. And the path length may be in limited in length, these were the big obstacles for collecting the data in particular time intervals. The purpose of using random collection at particular time intervals is the storage probability should be even with the dummy packet injection. Through this method of random data collection, this will greatly help to improve the secured transmission

REFERENCES

[1]. Albert, H., Robin, K., & Indranil, G. (2007). Building trees based on aggregation efficiency in sensor networks. Ad Hoc Networks,5(8), 1317–1328
[2]. Ergen,S.C.,&varaiya,p(2007),Energy efficient routing with delay guarantee for sensor networks, ACM wireless sensor networks.13(5)679-690.
[3]. Edith.C,.H.Ngai.Ioanna Rodhe(2012)On providing location privacy for mobile sinks in WSN.Wireless Networks(2013) 19:115–130.

[4]. . Lou, W., & Kwon, Y. (2006). H-SPREAD: A hybrid multipathscheme for secure and reliable data collection in wireless sensornetworks. IEEE Transactions on Vechicular Technology, 55(4),1320–1330.
[5]. Zhang, W., Cao, G., & La Porta, T. (2007). Data disseminationwith ring-based index for wireless sensor networks. IEEETransactions on Mobile Computing, 6(7), 832–847.
[6]. Ergen, S. C., & Varaiya, P. (2007). Energy efficient routing withdelay guarantee for sensor networks. ACM Wireless Networks.
[7]. Wang, W., Srinivasan, V., & Chua, K. C. (2005). Using mobile relays to prolong the lifetime of wireless sensor networks. In Proceedings of ACM Mobicom (pp. 270–283). New York, NY:ACM
.[8]. Lochert, C., Scheuermann, B., & Mauve, M. (2007, September). Probabilistic aggregation for data dissemination in vanets. In Proceedings of ACM VANET. Montreal, Quebec.
[9]. Rastogi, V., Suciu, D., & Hong, S. (2007). The boundary between privacy and utility in data publishing. In VLDB'07: Proceedings of the 33rd international conference on very large data bases(pp. 531–542).
[10]. Shah, R., Roy, S., Jain, S., & Brunette, W. (2003). Data mules: Modeling a three-tier architecture for sparse sensor networks. In Proceedings of IEEE international workshop on sensor network protocols and applications (pp. 30–41).

BIOGRAPHIES

N.Bhavya is received her B.Tech from Department of Information Technology, Arunai Engineering college tamilnadu, India and she is currently pursuing her M.E Computer Science & Engineering in Sri Krishna college of technology tamilnadu,India. Her area of interest is wireless sensor networks and Computer networks.

Ms.PL.Rajarajeswari is currently working as Assistant Professor in Sri Krishna College of Technology. She received her B.E from Department of Computer science & Engineering, Saranathan college of Engineering & technology, Tamilnadu, India. She did her M.E in Department of Computer science & Engineering, Sri Krishna college of Technology, Tamilnadu, India. Her area of interest is Computer Networks, Wireless sensor networks and Network Security.

Dr.N.K.Karthikeyan is currently working as Associate professor in Department of Information & Technology, Sri Krishna college Engineering & technology, Tamilnadu,India. His area of interest is a computer networks, mobile computing, Wireless sensor networks and High speed networks.