ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*Volume 3, Special Issue 3, March 2014*

**2014 International Conference on Innovations in Engineering and Technology (ICIET'14)**
**On 21st & 22nd March Organized by**

**K.L.N. College of Engineering, Madurai, Tamil Nadu, India**

# Improving Source Location Privacy Using Effective Localization in Sensor Networks.

[1]S.R.Naresh, [2]M.Abinaya, [3] Dr.A.V.Ramprasad

[1] Department Of ECE, KLN College Of Engineering, Sivagangai District, India.

[2] Department Of ECE, KLN College Of Engineering, Sivagangai District, India.

[3] Department Of ECE, KLN College Of Engineering, Sivagangai District, India.

**ABSTRACT**- Many protocols have been developed to provide privacy in wireless sensor networks. Contextual privacy is less concentrated in sensor networks compared to the content related privacy. Some technique provides data only from the local adversaries. In terms of well funded attacker, they can launch attacks such as back tracing and traffic analysis. To achieve source location privacy there is always a tradeoff between latency and location privacy. Proposed scheme focused on effective localization for improving source location privacy. Proposed algorithm uses the distance error calculation and proper refining of the location and periodical updating to the neighbors. Due to these procedures this method increases privacy in terms of latency and communication overhead. Through the Simulation and analysis, we exhibit that our proposed method is effective and efficient in protecting the source location privacy**.**

**KEYWORDS:** Source location privacy, Sensor networks, Localization, Context Privacy, Eaves Dropper.

## I.INTRODUCTION

Wireless sensor networks is the recent emerging technology, Challenges in this technologies are exclusive due to its different behavior .The sensor nodes are self-organize and self healing. Sensor nodes are grouped into a multi-hop wireless network that collects and forwards sensor data from source to a sink. These sensor nodes should provide three essential functions [2][3].
Corresponding author: nareshsr@yahoo.com

Ability to monitor physical and environmental conditions often in real times, its ability to operate device such as switches, and to provide secure and reliable communication.

General classifications of privacy threats are context-based and content-based [12]. Content-oriented privacy threats related to the message security and it is prevented using cryptography and encryption methods [4]. Even after these methods are applied, communication media still exposes contextual information.
From these information adversaries can extract sensitive information by analyzing the traffic pattern.

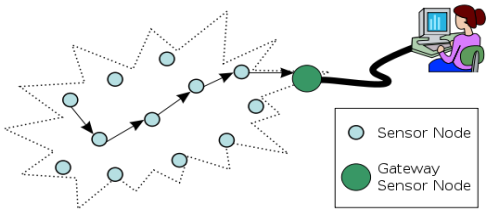


Fig 1: Wireless Sensor Network Model

Wireless sensor networks are widely used in many applications such as military applications, target tracking, Inventory tracking, etc., it also prevents the endangered species location privacy that has greater importance [6]. To detect the rare species like Siberian tiger sensor nodes are deployed randomly in an area which detect if there is presence and reported to the sink. Eavesdropper, here it refers to hunter may able to track the information and capture the tigers [8]. To avoid this, contextual information which contains the information about the source is prevented, which is the importance of source location privacy.

The paper is organized as follows, section II related work, section III network model, section IV proposed scheme, section V proposed algorithm and so on.

## II.RELATED WORK

Sensor network privacy has been studied in detail with some researchers giving significance in source location privacy by generating key [13]. Previous method provides source location privacy from global eavesdroppers. They assumes eavesdroppers are global and having the complete view of network traffic [1]. They also assume the sensor nodes are able to compromising. They also find out communication overhead needed to achieve some level of privacy and simulate their performances.

Some researchers used the techniques flooding technique and cyclic entrapment. Flooding technique method uses construction of numerous path through which the source can send the information to the sink. This makes it difficult for the adversary to trace the source [11].

Cyclic entrapment method creates loops at different places in sensor networks. This will cause the adversary to follow these loops repeatedly and thereby hide the source related information [9]. But this method causes wastage of energy and causes to down the lifetime of the sensors [4].

Another method named fake packet generation which creates fake source whenever sender notifies the real data to send [10]. Distance from fake node to the real node should optimize so that it could prevent location of source. These methods are trying to disguise the location information but with more energy overhead.

## III.EXISTING METHOD

In existing approach they used two techniques to hide the observed object periodic collection and source simulation [1]. Here periodic collection method provides optimum level of privacy but they send the packet at regular interval without considering whether real data to send or not [5]. A periodic collection method requires special hardware and this considerably increases the communication cost. Source simulation method is not highly suitable for the real time applications.

Primary reason for source location leakage was due to traffic pattern changes in the network. Eaves droppers will find out those traffic changes and detect the location of the source. One of the solutions to make traffic pattern independent for the real objects (events to be detected). To achieve this every sensor nodes in the network is periodically and independently send packets at regular interval regardless of whether real data to send or not.

Originally if any packets to be send to destination, then it sends the data that encrypts with the pair wise key. This key is shared with next hop and forwards it to that node. Otherwise it sends a dummy packet with payload, which is not authenticating correctly by the next hop. For energy consumption, additional communication used for hiding the traffic is needed.

Total No. of packet transmitted = $(T*N)/\Delta$

$\Delta$ indicates large amount of additional traffic. This means when amount of traffic increases this method is not suitable for the real scenarios. In terms of latency, there is a tradeoff between latency and energy consumption depending upon the value of $\Delta$. Thus the value of $\Delta$ should be optimized to improved latency and communication overhead. Source simulation method is not highly suitable for the real time applications [10]. This method uses the model like fake source generation with the distance far away from the real source [14] [15].

## IV.NETWORK MODEL

The sensor network is a homogeneous network consist of a sensors nodes that are spread over a large area. The incidence of events is sporadic and rare in nature. Number of unknown sensor nodes and beacon nodes are prefixed. The protocol used for this privacy purpose is AODV (Ad-hoc On Demand Vector). It is very simple and does not require any extra memory.

The simulation consists of 100 nodes, the location of which is randomly generated. All the nodes are deployed in 500m × 500m in radio propagation model. The radio range of the node is 100m. I have chosen initial energy as 2.0j and CBR as traffic agent. Transmitting and receiving antenna gain to be unity.

Adversary is considered to be non- intrusive, global eavesdropper and it is deployment aware. Adversary requires the information such as delay to find the location information.

## V.PROPOSED SCHEME

In terms of privacy none of the previous method can provide the location privacy under the assumption of the adversary as global eaves dropper. Thus source location privacy which is improved by localizing the actual sensor nodes accurately. By calculating the accurate position of the sensor nodes, source node can easily differentiate the active hops and non trusted nodes.

Proposed scheme can be used for many applications such as deployed in natural habitat to monitor the endangered species. In military this scheme is used in many monitoring applications. Here the scenario considered is, monitoring the endangered spice Siberian tiger in forest. In such application eavesdropper referred to hunter, trying to find the traffic pattern and find the source location and thereby he can easily determine where the event happens and can able to hunt the valuable species.

To avoid such situation effective localization scheme is preferred to provide security to the location information. The process of the proposed scheme is described using two process location requests and location response. Location request is sent to some of the selective reference nodes, which are replied with location response messages. The reference nodes will respond to the beacon nodes until their probability of accuracy is

higher than the required accuracy levels. Hence request from the eaves dropper nodes are ostracized by the reference nodes. Thus eavesdropper cannot able to mingle with normal nodes and cannot able to back trace the source node. After a proper request response session only normal nodes get authenticated and location information can be send via those nodes and eavesdropper nodes can be found out and thus prevent launching of any traffic analysis attack by the spy nodes.

## VI.PROPOSED ALGORITHM

*A.Initialization*

This phase includes broadcasting location request to the selective reference nodes and which in turns return response message to the unknown or normal nodes.

*B.Initial position estimation*

In this phase two parts takes place. In first part they use smart reference Selection method to select few reference nodes having high probability of accuracy. In second part, it measure the distance to each reference. By using those it finds the initial nodes position.

*C.Refined position estimation*

This is the third phase of the algorithm which enhances the accuracy of the position estimation of the nodes by considering the distance error.

$$e_{i,j}^{d} = \left| \P\hat{z_i} - \hat{z_j}\P - \hat{d_{i,j}} \right|$$

$e_{i,j}^{d}$ is the estimated distance error. This is the difference between the calculated distance and the measured distance ($\hat{d_{i,j}}$). Here calculated distance is the values between node's initial position ($\hat{z_i}$)and the reference position ($\hat{z_j}$). By using this equation, node with distance errors are estimated. Thus estimated nodes are not selected as the reference node. Other node in the list is eliminated to be the reference node.

*D.Position update*

In this phase it checks for the above procedure and found out the final estimation position and applies the termination criterion.

When compared to the existing system, the proposed scheme ensures low energy overhead and reduced delay and having reasonable trade-off with the energy consumption.

## VII.SIMULATION

The performance of the sensor nodes are demonstrated through NS2 tool. The simulation scenario had deployed 100 nodes. Out of 100 nodes 12 nodes are considered to be spy nodes for understanding the simulation scenario. Initially normal nodes are marked as yellow and eavesdropper nodes as blue nodes.

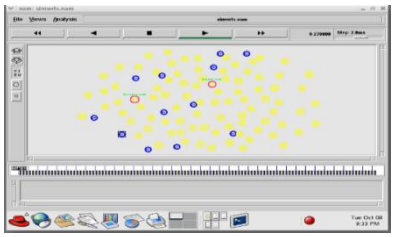

Fig 2: Initial node placement

Fig 2 shows broadcasting of location request message to the reference nodes in their neighboring list. The reference nodes will send the response message to the corresponding nodes.

After the nodes get authenticated, the nodes are considered as trusted nodes. Hence location information was transmitted only to the trusted nodes and prevents the location information from leaking to the eavesdropper or malicious nodes. The circle indicates broadcasting of request and response message.

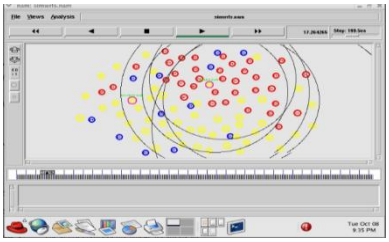

Fig 3: location request-response

After completing the request-response session, the nodes' having high probability of accuracy is only responded and turns out to red color. Eaves dropping nodes are remaining in the same blue. Hence location information cannot leak to the spy nodes.

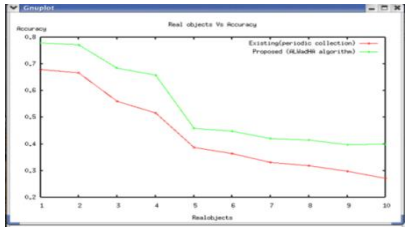

Fig 4: real objects Vs accuracy

Fig 4 shows, the calculation of accuracy value depends upon the number of events to be detected (real objects). The accuracy value is compared between existing and proposed system.

In this proposed method, number of events to be detected decreases, throughput of the corresponding nodes increases. This is depending upon the highest level of accuracy. This shows efficiency is also increased.

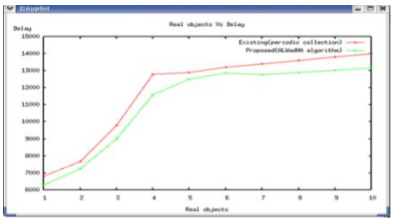

Fig 5: real objects Vs delay

Latency here refers to the delay in sending the information from source to destination without interuption of eavesdropper showed in fig 5. Here events to be detected (real objects) increases delay also increased. Thus if delay was reduced then the communication cost is also reduced, lifetime of the active nodes is also increased.

## VIII. CONCLUSION

Though lots of protocol provides privacy for the content of the message, contextual privacy is less concentrated in security issues. Some researchers found some technique for source location privacy. In terms of well motivated attacker there is always tradeoff between latency and privacy. Proposed scheme focused on effective localization algorithm which increases the privacy of source location. Since this algorithm uses the distance error calculation and proper refining of the location and periodical updating to the neighbors. This method increases privacy in terms of communication overhead and latency. Our proposed scheme is reduces the above parameters since this method avoids transmission of dummy packets as in case of existing method. Simulation and plotted graph results shows that our proposed method is effective and efficient in protecting the source location privacy. Future work is to improve the location privacy including sink nodes in the network and analyzing the parameters such as overhead, latency and communication cost.

## REFERENCES.


[1] Kiran Mehta, Donggang Liu, and Matthew Wright*" protecting location privacy in sensor networks against a global eavesdropper*" Member, IEEE, IEEE transaction on mobile computing , vol .11, No.2, pp.February 2012.

[2] M. Mahmud and X. Shen, "*Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks*," Proc. IEEE INFOCOM '11-Int'l Workshop Security in Computers, Networking, and Comm. (SCNC), pp. 1006-1011, Apr. 2011

[3] K. Bicakci, H. Gultekin, B. Tavli, and I.E. Bagci, "*Maximizing Lifetime of Event-Unobservable Wireless Sensor Networks*," Computer Standards and Interfaces, vol. 33, no. 4, pp. 401-410, June2011.

[4] H. Wang, B. Sheng, and Q. Li, "*Privacy-Aware Routing in Sensor Networks*," Computer Networks, vol. 53, no. 9, pp. 1512-1529, 2009.

[5]Dong gang Liu, Peng Ning, An Liu, Cliff Wang, Wenliang Du, "*Attack- Resistant Location Estimation in Wireless Sensor Networks*", in *ACM Transactions in Information and Systems Security (TISSEC)*, 2008.

[6] K. Sohraby, D. Minoli, and T. Znati, Wireless Sensor Networks: Technology, Protocols and Applications. John Wiley & Sons, Inc., 2007.

[7] J. Deng, R. Han, and S. Mishra, "*Decor relating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks*," Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

[8] Y. Zhang, W. Liu, W. Lou*, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks*," IEEE J. Selected Areas Comm., vol. 24, no. 2, pp. Feb. 2006.

[9] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "*Entrapping Adversaries for Source Protection in Sensor Networks,"* Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.

[10] "Kamat, Pandurang; Zhang, Y.; Trappe, W.;
Ozturk, C., "*Enhancing Source-Location Privacy inSensor Network Routing*," *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on* , vol., no., pp.599,608, 10-10 June 2005.

[11] C. Ozturk, Y. Zhang, and W. Trappe, "*SourceLocation Privacy in Energy-Constrained Sensor Network Routing*," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.

[12] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy, "*The platforms enabling wireless sensor networks*," Commun. ACM, vol. 47, no. 6, pp. 41-46, 2004.

[13] D. Liu and P. Ning, "*Establishing pairwise keyin distributed sensor networks*," in Proceedingsof10thACM Conference on Computer and Communications Security (CCS), October 2003, pp. 52-61.

[14] J. Deng., R. Han, and S. Mishra,"*Enhancing base station security in wireless sensor networks*,"2003. [Online]. Available: citeseer.ist.psu.edu/deng03enhancing.html

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "*SPINS: Security protocols for sensor networks*," in Proceedings of Seventh Annual International Conference on Mobile Computing and Networks (MobiCom), July 2001.