Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Wireless Sensor Network Location Privacy based on Hybrid Approach by Source Simulation & Confused Area

Pushpa Sahu
M.Tech Computer Science (Multimedia Technology)
Kalinga University Raipur (C.G.) India

Mr. Mohammed Bakhtawar Ahmed
Assistant professor
Computer Science Department
Kalinga University Raipur (CG) India

***Abstract*—Wireless sensor systems are generally utilized as a part of our day by day life. It comprises of different sensors which gather distinctive data containing the personality, status, and area of an item or some other business, social or secretly applicable data. However, we pay consideration on a few issues identified with sensor's area security or sensor's location privacy. In this paper, we concentrate on ensuring the sensor's area by acquainting suitable adjustments with sensor directing to make it troublesome for a meddler to locate the first area. And we propose a Hybrid Approach by Source Simulation & Confused Area Scheme, which is a flexible routing strategy to protect the sensor's location. Our technique can effectively diminish the possibility of bundles being recognized. Also, the foe can think that it's hard to locate the accurate area of the source hub or the base station. In our task confused area scheme as well as source simulation method are utilized. So if an enemy is break the security conspire so another system arrives to ensure the sensor area. By along these lines we can all the more viably secure the sensor's area.**

Keywords— WSN; Preserving Privacy; Sensor's Location; Confused Areas, Source Simulation.

I. INTRODUCTION

Remote sensor systems have increased more notoriety as of late. In remote sensor systems, sensors are conveyed in different sorts of utilizations to screen occasions furthermore, Transmit data to base station. In battlefield, sensors are conveyed to screen adversary's movement and send messages to base station, Furthermore, sensors can likewise be conveyed to screen nature and temperature in non military personnel applications or screen creatures in normal natural surroundings. In war zone, sensors are sent to screen foe's movement and send messages to base station. What's more, sensors can likewise be conveyed to screen the earth and temperature in non military personnel applications or screen creatures in characteristic natural surroundings [1]. In wireless sensor networks, sensors are easy and convenient to collect information. But an obvious challenge that is a possible danger to deploy sensor networks successfully is privacy. For instance, a sensor detects an object, sending a message including event related information to the sink or the base station [2]. On the off chance that a busybody can capture the message, he may know some delicate data that where and when a concerned occasion has happened by watching and dissecting the message. Thus, the meddler may locate the precise area of the article and control or decimate the item, which is a risk to the entire Wireless sensor system. So Location protection is an essential security issue. Truth be told, virtual data has a corresponding association with genuine elements in personality data. In the event that area protection is revealed by an enemy, some personality data may be Uncovered [3]. As we probably am aware, area data regularly implies the physical area of the occasion, which is urgently given some utilizations of remote sensor systems [4]. In this manner, at the point when an aggressor gets area data by breaking down a message that was caught, he will move to the area and screen the occasion. At that points the aggressor will gather bunches of private data and assault the exceptional hubs.

In this paper, we subscribed hybrid approach of Confused Areas method as well as the Source Simulation Scheme to preserve sensor location information in wireless sensor networks. The confused areas consist of a given number of sensor nodes in wireless sensor network. Sensors which are located on each initial area will serve as the receptors. And each sensor will store its neighbors in the same area. When sensor node receives a packet in an initial area, the node will broadcast the packet to its neighbors and randomly choose one neighbor to send the packet. Then a packet is randomly forwarded from a source until it reaches an initial area. In the area, the node broadcast the packet to its neighbors and one of its neighbors sends the packet to another node. And then the packet is randomly forwarded again until it reaches the sink. The packet is randomly forwarded so that it is difficult to detect the packet by an eavesdropper. Even though an eavesdropper happens to detect a packet, the next packet is unlikely to follow the same path, thus rendering the previous observation useless. So the Confused Areas can efficiently protect the source node and base station.

In the source simulation approach, an arrangement of fake sources will be reenacted in the field. Each of them generates a traffic pattern similar to that of a real object to confuse the adversary. Fake packet generation [5] creates fake sources whenever a sender notifies the sink that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the sink as the real sender

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Whatever is left of the paper is sorted out as take after. Related work and already proposed strategies for area protection are exhibited in Section II. After that, Section III presents different techniques that we subscribed in this paper that is confused area and source simulation method. In section IV performance of different method are evaluated as well as different location privacy techniques are compared with each other and expected result are shown in tabular form. At long last, we concluded this paper in Section V.

II. RELATED WORK

In remote sensor systems, sensors may be conveyed in regular natural surroundings to screen creatures, or be utilized as a part of war zone to screen foe's action and send messages to base station. So it is critical to give privacy to the source sensor's area.

Panda-Hunter Game is proposed in [6], which is an application situation of a remote sensor system for observing a panda.

In this amusement, countless sensors are conveyed in a panda living space. At the point when sensors have watched a panda, they will produce occasion messages and send them to the base station. In the interim, a panda-seeker tries to catch the panda by back-following the directing way until it achieves the source. In this manner, a safe directing plan ought to keep the seeker from finding the source, while transmitting the information to the base station. For the area data of sensors, Random walk can effectively protect sensor's area security. A message is haphazardly sent from source, while it does not uncover any data about the source really, an enemy can't know which arbitrary way the exact course is. So he can't discover the area of source and potentially achieve an obscure sensor. Be that as it may, an immaculate arbitrary walk plan is not secure for saving private data of the area [5]. What's more, it can be demonstrated that an unadulterated arbitrary walk tends to stay around the genuine source [7]. Phantom Routing is proposed in [5], which is one of arbitrary walk approaches. The phantom is utilized to transmit data from the area of the panda to the sink for safeguarding its area security. Firstly, a message is arbitrarily sent a couple ventures from information source. And after that, the message is being conveyed through flooding or single way directing to base station. And it is vividly shown in Figure 1.

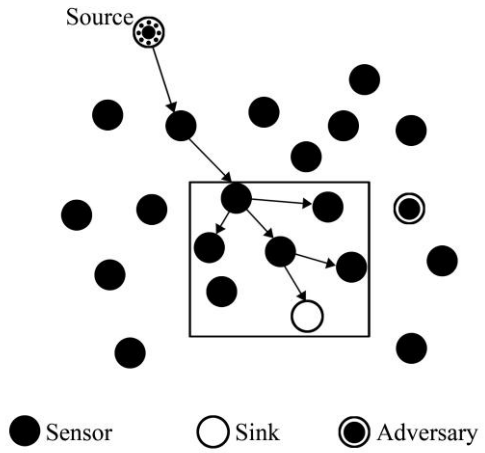

Fig 1. Phantom Flooding protocol

Greedy Random Walk situation is proposed in [4]. Firstly, it is started an irregular way with a given number of jumps from the sink. At that point every sensor on the way gets message as a receptor. Every message is arbitrarily sent from a source until it achieves a receptor. And after that the message is sent to the sink through the pre-built up way. In any case, an enemy still potentially back trace to a sensor. What's more, if a spy can screen the entire sensor system, he may watch and examine all movement transmitted in the remote sensor system [8]. Furthermore, at that point he will find that the movement is higher than different sensors in this way. Subsequently, the busybody may discover the pre-established way and forward to base station through the pre-established way in that point. So it may debilitate the security of the base station.

Cyclic Entrapment is proposed in [9], which is an methodology of loops of messages. And fig 2 shows the cyclic entrapment scheme. A few traps are set to the foe on his way to the source in the strategy. In the traps, bait messages are sent in a roundabout manner to keep the foe far from the source. Furthermore, the nodes choose whether to produce a circle taking into account some likelihood. At the point when one of the circle actuation hubs gets a genuine information parcel, a circle is activated. At the point when the foes follow back to the source hub, they will settle on a choice to pick the following jump at the initiation hubs. The skilled adversaries avoid the loop to prevent to trap in circle or loop.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

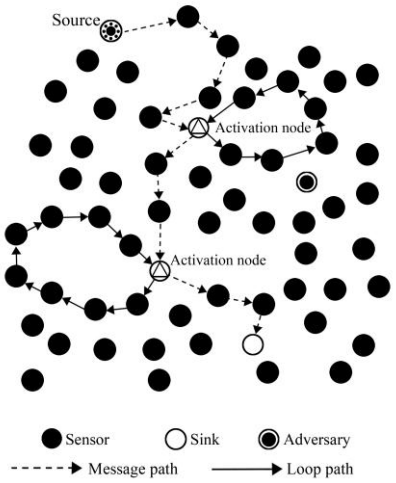

Fig 2.Cyclic Entrapment Method

Fake packet generation process [5] makes fake sources at whatever point a sender tells the sink that it has genuine information to send. The fake senders are far from the genuine source and roughly at the same separation from the sink as the genuine sender.

III. Depiction of different techniques:-

Confused area scheme:-

Albeit numerous current security procedures can be utilized in sensor system situations, they can't adequately keep the foe from discovering the area data of source or base station. So keeping in mind the end goal to safeguard data of area security, we propose a Confused Territories plan to address this issue.

Protocol description:-

In this plan, we arbitrarily start a few territories which comprise of a given number of sensor hubs in remote sensor system. Sensors which are situated on every introductory range will serve as the receptors. What's more, every sensor will store its neighbors in the same territory. At the point when a sensor hub gets a parcel in an introductory range, the hub will show the bundle to its neighbors and arbitrarily pick one neighbor to send the bundle. At that point a parcel is arbitrarily sent from a source until it achieves an introductory territory. In the range, the hub show the parcel to its neighbors and one of its neighbors sends the bundle to another hub. And after that the bundle is arbitrarily sent again until it achieves the sink. Along these lines, the starting territories call the befuddled regions. Figure 3 shows the essential thought of Confused Areas. Then again, it is conceivable that a bundle may forward to one of its past bounce's neighbors or confounded territories. So such that sending plan is bad since the arbitrary walk does not gain much ground. Also, the sensor hubs have its channel pool and store the sending parcel data in the channel.

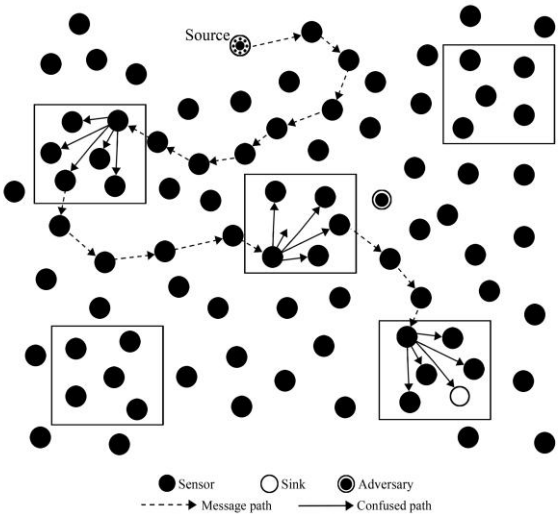

Fig 3. Confused area scheme

At the point when a sensor arbitrarily picks next bounce from its neighbors, it ought to check whether the neighbor has been as of now in the channel. On the off chance that the neighbor isn't in the channel, the sensor will telecast the following hub's ID to other sensor hubs. At that point different hubs store the following sensor's ID in the channel.

Confused Area Algorithm

Algorithm: Confused Area Strategy
current_location = source;
next_location = ChooseNeighbors(current_location);
filter;
packetInfo;
current_node;
is_confused_area_sender=false;
while (next_ location!= sink) ***do***
if(!(current_location in confused area)) ***then***
if(!(next_location in filter)) ***then***
if(next_location in confused area) ***then***
is_confused_area_sender=true;
else
is_confused_area_sender=false;
end if
MoveTo(next_location, packetInfo,
is_confused_area_sender);
else
next_location=ChooseNeighbors(current_location);
end if
else
if(is_confused_area_sender) ***then***
is_confused_area_sender=false;
SendMsgToAllNeighbors(packetInfo,
is_confused_area_sender);
else
next_location=ChooseNeighbors(current_location);
MoveTo(next_location, packetInfo,
is_confused_area_sender);
end if
end if
filter=StoreSensorsInfo(current_location);
end while

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

As is appeared in Algorithm 1, a bundle will be sent to base station by Confused Area strategy. The bundle is sent from the source that haphazardly picks its neighbor as the next bounce. At that point the parcel is sent to the following hub. In the event that the hub is in the befuddled zone, the hub will transmit a parcel to its neighbors in the same territory. Something else, if the hub is not in the confounded range, the hub will haphazardly pick its neighbors. At that point if the bundle is not in the channel, the channel will store the data of the bundle in this hub. Each hub takes after the principle to send the parcel until it achieves the sink. Note that it is effective to safeguard the sensor area protection in our plan. The bundle is haphazardly sent so that it is hard to distinguish a bundle by a spy. What's more, the hubs in the befuddled zone telecast the parcel to its neighbors and arbitrarily pick the following bounce. The enemy can't accurately identify a bundle which is transmitted by confounded hub. Despite the fact that a busybody happens to recognize a bundle, the following parcel is unrealistic to take after the same way, in this manner rendering the past perception pointless.

Source simulation

In this scheme we establish make various applicants follows in the system to shroud the movement created by genuine items. Instructions to decide the quantity of competitor follows is application subordinate. Making competitor follows in the field is entirely testing by and by. The fundamental issue lies in the trouble of displaying the conduct of a genuine object in the field. An inadequately planned model will probably fall flat in giving security insurance. For instance, as appeared in Fig. 4, the conduct of fake articles is demonstrated mistakenly as staying in one area constantly. In light of this model, the applicant follows are made at areas (F1; F2; . . . ; F6).

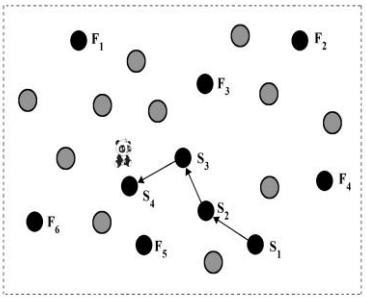

Fig-4. Leakage of location information

Sensors at each of these areas will send fake activity to the sink, reenacting a genuine item. On the other hand, the enemy can just notice that the article moves around in the field along the way fS1; S2; S3; S4g and use this additional learning to recognize genuine articles from fake ones. When all is said in done, the assailant may have the capacity to recognize the development examples of genuine articles from fake ones, regardless of the fact that we have the fake ones move. Luckily, much of the time, a foe won't have Significantly more learning about the conduct of genuine objects than the shield. Luckily, much of the time, a foe won't have significantly more learning about the conduct of genuine objects than the shield. In this manner, it is regularly sensible to accept that the foe and the guard have comparable learning about the conduct of genuine items. We can then create more useful candidate traces in the field to hide real objects.

Protocol description:-

In the source simulation approach, an arrangement of fake articles will be recreated in the field. Each of them produces an activity design like that of a genuine item to confound the enemy.

Source recreation functions as takes after: before organization, we haphazardly select a set of number of fake sources of sensor hubs and preload each of them with an alternate token. Each token has its unique ID. These tokens will be gone around between sensor hubs to recreate the conduct of genuine articles. For accommodation, we call the hub holding a token the token hub. After organization, each token hub will transmit a sign imitating the sign utilized by genuine articles for occasion location. This will trigger occasion discovery in the neighborhood .what's more, create movement as though a genuine occasion was distinguished. The token hub will then figure out who in its neighborhood (counting itself) ought to run the following round of source reenactment in view of the conduct profile of genuine articles. The token will then be gone to the chose hub. The conveyance of the token between sensor hubs will dependably be ensured by the pair wise key built up between them.

IV. PERFORMANCE EVOLUTION

In this section we evaluate the performance and privacy protection level of subscribed method.

Table 1 demonstrates the latency of bundle conveyance when there are various pandas. We can see that as the quantity of pandas expands the idleness increments means latency increases. This is on the grounds that the nodes near the base station get numerous reports in the meantime, which obliges them to cradle the bundles. At the point when the quantity of pandas develops too huge, the buffered packet being dropped because of the constrained size of the queue, and the latency of the bundles that do touch base at the base station gets to be steady after a certain point. At the point when the queue size q diminishes, packets Voyaging long separations have a high likelihood of getting dropped, making the latency of the packets that do arrive at the base station littler. This can be seen by a drop in the latency for littler estimations of q in the table.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Table -1
Latency of packet delivery with respect to multiple panda

No of panda	Latency Per Packet in Term of Time Interval		
	Queue size=1	Queue size=5	Queue size=20
5	5	5	5
10	4.99	6	6.1
20	4.91	7	8
30	4.89	7.5	11
40	4.87	8	14
50	4.85	8.2	16
60	4.8	8.5	17
70	4.78	8.7	19
80	4.75	9	20.5
90	4.75	10	22.5

Table 2 demonstrates the rate of the distinguished percentage gotten by the base station. We can see that the rate of percentage got diminishes when there are more pandas in the field. Expanding q will absolutely build the rate of the occasions sent to the base station. Be that as it may, after a certain point, expanding q won't generously raise the bundle drop rate, as seen by the little contrast from when q=5 to q = 20. Then again, we see from table 1 that expanding q will essentially build the inertness of parcel delivery. Consequently, genuinely little estimations of q will typically show the best exchange off point between parcel drops and inactivity. By and large, the outcomes in table 1 and table 2 give a rule for designing the line size q to meet different necessities.

Table-2
Event Detected W.R.T. panda

No of panda	percentage of event detected by the base station in %		
	Queue size=1	Queue size=5	Queue size=20
5	95	100	100
10	88	100	100
20	72	98	99
30	65	88	90
40	57	78	80
50	52	75	76
60	48	69	70
70	45	64	65
80	40	59.5	60
90	38	67	68

Comparison:-

We now look at the source-location protection approaches in this paper with two other security protecting procedures**.** The consequence of our reenactments is appeared in Fig.5. The overhead of the ghost single-path scheme. Overheads of the periodic collection and the proxy based separating procedures are spoken to by focus on the right some portion of the table3. Table 3 additionally demonstrates the correspondence costs included in distinctive systems. The reenactment results are as we would foresee from instinct.

The ghost single-way steering procedure presents generally little correspondence overhead, while the occasional gathering System includes noteworthy in any case, consistent correspondence cost for a given period of time. The reenactment results are as we would foresee from instinct. The phantom single-path steering procedure presents generally little correspondence overhead, while the periodic collection system includes noteworthy in any case, consistent correspondence cost for a given period of time. The reason is that the source simulation method is arranged to bolster continuous applications with a period interim.

From the table 3 it is clear that the communication cost of proxy based filtering is in among periodic collection and TSM Algorithm. amid recreation of PFS method, we saw that around 70 percent of event were gotten by the base station.

Table-3
Communication Cost of Different method W.R.T. No of Bits

Privacy in terms of bits	Communication Cost of Different Method			
	Source simulation	Periodic collection	Phantom Single Path(PFS)	TMS tree algo
1	$10^{0.4}$	$10^{0.3}$	$10^{0.3}$	$10^{0.1}$
2	$10^{0.6}$	$10^{0.5}$	$10^{0.4}$	$10^{0.4}$
3	$10^{0.9}$	$10^{0.7}$	$10^{0.6}$	$10^{0.5}$
4	$10^{1.2}$	10^{1}	$10^{0.9}$	$10^{0.7}$
5	$10^{1.5}$	$10^{1.3}$	$10^{1.25}$	$10^{0.8}$
6	$10^{1.7}$	$10^{1.5}$	$10^{1.3}$	$10^{0.9}$
7	10^{2}	$10^{1.7}$	$10^{1.6}$	10^{1}
8	$10^{2.4}$	$10^{1.9}$	$10^{1.8}$	$10^{1.2}$
9	$10^{2.5}$	10^{2}	$10^{1.9}$	$10^{1.4}$
10	$10^{2.8}$	$10^{2.3}$	$10^{2.1}$	$10^{1.6}$
11	10^{3}	$10^{2.5}$	$10^{2.2}$	$10^{1.9}$
12	$10^{3.7}$	$10^{2.7}$	$10^{2.6}$	$10^{2.1}$

The outcomes are appeared in table 4 the source simulation method can give commonsense tradeoffs between area protection and correspondence cost.

In expansion, in view of table 4 we can obviously see that the source simulation thought can accomplish a superior discovery rate when the protection prerequisite is b =6 or less bits.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Table -4
Percentage of Event Received by source Simulation

Privacy in bits	% of Event Received
2	100
4	100
6	90
8	30
10	15

V. CONCLUSION

Remote sensor system is generally sent to gather important data in our everyday life. However, it is obvious that preserving private location information is a big challenge in sensor network. And an eavesdropper may be able to find location information by monitoring and analyzing message routing paths, which can be a serious privacy issue. In this paper, we propose Confused Areas & Source Simulation to keep a adversary from backtracking message Routing path to the Event source or breaking down the transmitted ways to locate the base station, which can upgrade the protection assurance. Also, it can proficiently ensure the area. And it can efficiently protect the location information of the source nodes and the base station. Our future work is to further study wireless sensor networks and efficiently protect location privacy

VI. REFERENCES

[1] Rios, R. and Lopez, J. “Analysis of location privacy solutions in wireless sensor networks”, IET Communications, Vol. 5, 2011, pp.2518-2532.
[2] Rios, R. and Lopez, J. “Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks”, TheComputer Journal, Vol. 54, 2011, pp.1603-1615.
[3] Chuang, P.J., Deng, J.S. and Lin, C.S. “Location Privacy ProtectionUsing Independent ID Update for WLANs”, Journal of InformationScience and Engineering, Vol. 27, 2011, pp.403-418.
[4] Yong, X., Schwiebert, L. and Weisong, S., “Preserving source location privacy in monitoring-based wireless sensor networks”, In Proceedings of the 20th International Parallel and Distributed Processing Symposium, 2006, 8 pp.
[5] Kamat, P., Zhang Y.Y., Trappe, W. and Ozturk, C., “Enhancing Source-Location Privacy in Sensor Network Routing”, In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, 2005, pp.599-608.
[6] Ozturk, C., Zhang, Y.Y. and Trappe, W., “Source-location privacy inenergy-constrained sensor network routing”, In Proceedings of the2nd ACM workshop on Security of ad hoc and sensor networks, 2004, pp.88-93.
[7] Li, N., Zhang, N., Das, S.K. and Thuraisingham, B., “Privacy preservation in wireless sensor network: A state-of-the-art survey”, Ad Hoc Networks, Vol.7, 2009, pp.1501-1514.
[8] Mehta, K., Liu, D.G. and Wright, M., “Location privacy in sensornetworks against a global eavesdropper”, In Proceedings of the IEEE International Conference on Network Protocols, 2007, pp.314-323.
[9] Ouyang, Y., Le, Z., Chen, G., Ford, J., Makedon, F., “Entrappingadversaries for source protection in sensor networks”, WOWMOM’06: Proc. 2006 Int. Symp. On World of Wireless,Mobile and Multimedia Networks, 2006, pp.314-323.