The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 2 || Pages || PP -16-22|| 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Realistic adversary model for mitigating hotspot locating attack based privacy preserving scheme in Wirelesssensor network

[1]S. Saravanan , [2]Dr. M. Prabakaran
[1]*Research Scholar, Assistant Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamilnadu, India.*
[2]*Research Advisor, Assistant Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamilnadu, India.*

----------ABSTRACT----------

Wireless sensor network (WSN) consists of a large number of sensing devices which are called sensor nodes and they are interconnected through wireless links to perform distributed sensing tasks. The source using the data collector in network, data collector is called as Sink. This data transmission may occur through Multihop transmission, where the sensor nodes act as routers. Since the sensed data are typically transmitted through wireless channels, so adversaries can easily eavesdrop the information about location of source nodes.In this paper we develop a realistic adversary model which can monitor multiple parts of thenetwork and can analyze the traffic in those areas. Next we propose anattack based privacy preserving scheme by creating fake traffic ofirregular shape which provides an efficient mechanism to protect the source node's location in addition to that we also generate the fakepacket at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with theinconsistencies in the network. Next we are introducing the concept of context aware location privacy where the sensor nodes are havingthe ability to perceive the presence of adversary in their vicinity in order to transmit data packets in more energy-efficient manner.

Keywords: *Data collector, Sink,Context Aware Location Privacy, WSN.*

Date of Submission: 13 January 2016 Date of Accepted: 05 February 2016

I. INTRODUCTION

Wireless sensor network contain of insignificant, multifunctional and reserveforced sensors. Every time sensor node identifiesathing it may be fighter in military request andcommonphysical in case of environment monitoring it intelligencesthat event to the sink which is a commanding data collectionunit. In this paper we consider environment monitoringrequest where the devices are used to monitor the nodes, for instance a WSN consume been organized tomonitor the all foundation based location.The sensors infrequently sense the data of theiroccurrence and activities and the detected data is described tothe sink. However, WSN are positioned in large and openareas so that providing corporal boundary or appearingeach sensor node grow into almost impossible.

While theinfo is sent from foundation to the sink finished thebroadcast link, the adversaries can eavesdrop on thewireless medium and container locate the source nodes bycreation use of traffic gen to the network.Therefore it is important to preserve the foundation node'slocation because of the acceptance of locating hotspot andtheir furs big market value.In the international adversary founded scheme the adversary hasthe competence to monitor the each radio transmission andthe links among them. In this structure it is it is expectedthat adversary can monitor the complete network which isimpracticable in large areas.

Adversary is having international viewof the network incomes that the assailant can locate node without the use of network transmissions.Wedetermination study the hotspotoccurrence in which challenger tries to discover the hotspot byanalyzing the traffic evidence collected by theintensive care devices. Adversary follows the traffic investigationtechniques such as time associations, packet relationshipsand nodes sending rates to find the hotspot. Finally wepropose our hotspot based context aware scheme in which we make a detection offake traffic in adding to that we also make the fakeevent at a specific time interval so that opponent cannotassociate the expected hotspot regions similarsink node with the variations in the network to break theincompatibility in the traffic pattern produced by hotspot tocomplicate the source node inside the collection of nodes.

Hereto decrease the energy consumption of conducting nodeswe remain using context-aware location privacy approach. Its revenues advantage of sensor nodes context-awareness in order to identify the attendance of amobile opponent in their environs so that packages aredirected in a more well-organized and confidentiality preserving manner.The solution aims to expect the actions of theattacker in instruction to reduce the number of packets isable to detention and analyses, hence dropping the likelihoodof the attacker discovery the source.

II. RELATED WORKS:

The MPRA to perform routing of data packet and acknowledgement. The source node chooses its own path to transmit the packet to the destination where the destination node selects a different path than the data packet followed to deliver the acknowledgement. The selection of reverse path is performed according to the location of the source node. To perform such routing the popular Location Aided Routing is used. Every source node to send data in to neighbor's node or sink node. The sink nodes are used the position Aided Routing technique. And all and each node decides the way of broadcast. In these broadcast basses on the time [1].

Each source assign in to dissimilar time slot. Between the times every sources node sends the in sequence in to equivalent destination node. Location is based to more often than not put into practice the capital from necessary logic purpose on the process.The secured logging as a service in hotspot architecture. So in theproposed method, privacy and preservation methods are enhanced. The secured logging contains six majorfunctionalities to ensure more securities: Correctness, Confidentiality, and data logs, Privacy, Preservation and virtual proxy server [2]. The correctness deals with correctness data of the true history. Confidentiality dealswith sensitive information not displaying during search.

Data logs deals with the data history for identifyingappropriate users. Privacy scheme deals with file linking and data access history. Preservation deals withenhanced color code. And finally virtual proxy server deals with the proxy server for virtual data access [4, 5]. Virtual proxy server development of mobile ad hoc networks has stimulated numerous wireless applications that can be used in awide number of areas such as commerce, emergency services, military, education, and entertainment.The network can leakconfidential data, modify the data, or return inconsistent data to different users.

This may happen due to bugs,crashes, operator errors, or misconfigurations. Further-more, malicious security breaches can be much harder todetect or more damaging than accidental ones: external adversaries may penetrate the data storage provider, oremployees of the service provider may commit an insider attack [6, 7]. These concerns have prevented securityconsciousenterprises and consumers from using the data regardless of its benefits. A hotspot is formed when the more number of packets arises from the small area.

Packets there may be traffic in the network. Through this the adversary can try to learn the data [9]. To avoid this problem the packets are send in the form of the network with irregular shapes which makes inconsistency to the adversary to track the data from network. The adversary randomly distributes the devices for monitoring the data transmission. If adversary finds the area but there is no animal say panda, then it is known as the false positive. However the adversaries are well equipped to track the data during the transmission [10].

III. PROPOSED SYSTEM:

The wireless sensor network contains of sink then large noof sensor nodes organized in the intensive care area which arehaving the aptitudes to detect a hotspot. The source nodeand sink are stationary. The sensor nodes have incompletebattery power, addition capacity and limited networkannouncement bandwidth. Each sensor node is equippedwith sensing device, data processing and interactivecomponents.The sink has enough computation and storingcapabilities to achieve the functions:

1) Broadcastingbeacon packets to bootstrap our scheme.
2) Collecting thedata sensed by the sensor nodes.

Hotspot have surroundedradio incidence tags and as soon as sensor node senses ahotspot, the node is called source node which refers eventpacket to the sink.

3.1 Attack discovery-Based Scheme for Adversary Model:

Anattack discovery based scheme for defensive source nodes location. It reservation the privacy compared to hotspot-locating attack by making a data collector with an uneven shape of fake traffic and a group of nodes founding the network. The fake packet also enable the real source node to send the sensed data to a fake area node that have designated from the grouping nodes and it send to the sink. Sink is the network to accept and send the data. The sending and receiving data can be encoded using cryptographic method. This

processes are used to alteration the packets arrival at each place then it helps to avoid the packet association and make the source node in network. Because the adversary model to differentiate the fake data and real traffic data. When the statistics is sent on or after source to the destination the challenger can eavesdrop on the frequency and can locate the foundation of the information to control the location of network.

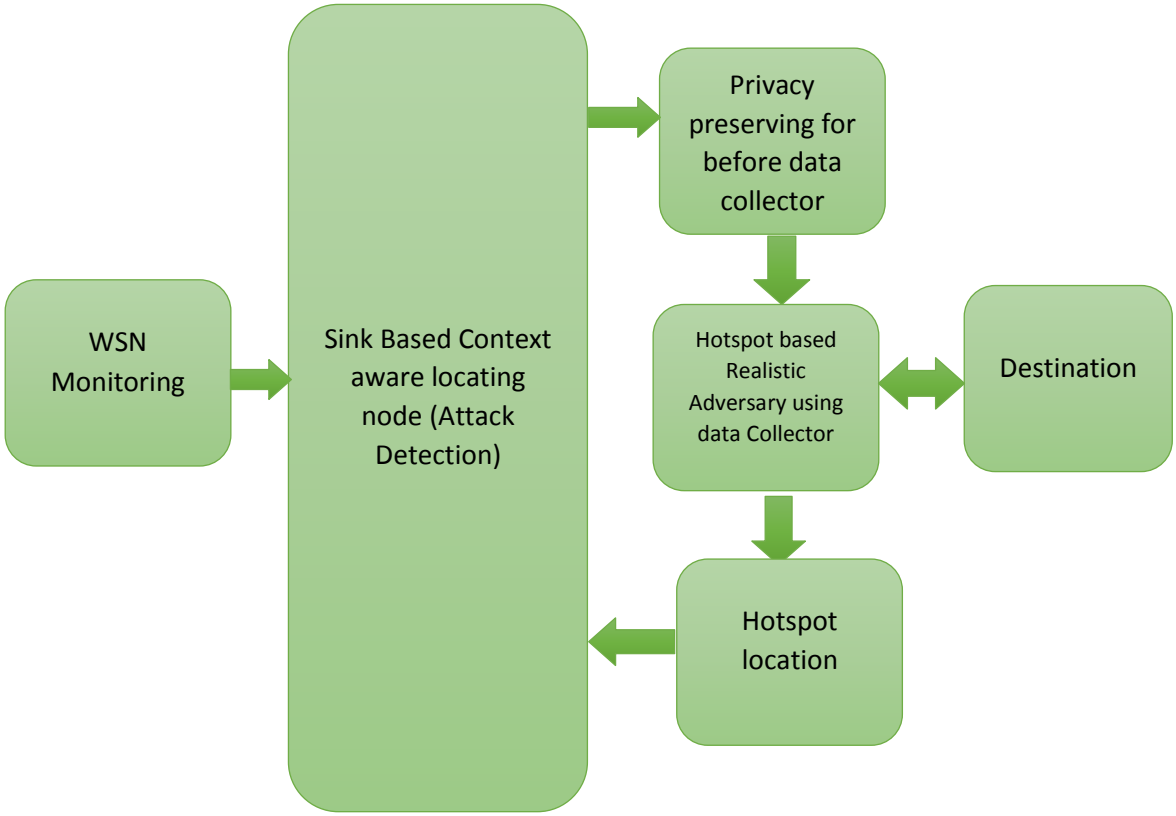


Figure 3.1 Proposed Flow Architecture Diagram

The adversary distributes the number of checking devices in the absorbed region to collect the traffic information in these areas but it cannot monitor the whole network. The adversary is inactive and does not involve through the active attacks to continue hidden from the network operator. Each monitoring device contains of spectrum analyser and antenna. The attacker can interrupt the packet and can measure the angle of entrance and received signal strength to determine the location of the node.

3.2Context Aware Location Privacybased Hotspot Locating:

A Context Aware Location Privacyis produced, when after small area large statisticsof packages are sent since sensor node which causesindiscretion in the linkage so that enemy makes use ofthese changeability in the network.

Algorithm for Hotspot Locating Attack:

Start
Network monitor
Examine the data collector
While
(To redirect hotspot location),
Do
Flooding on the data packet and Hotspot position
If hotspot is find the correct destination
To transfer the data in source to destination
Else
Alteration the position of the observing device
End

The traffic analysis techniques such as content correlation,time correlation and packet sending rates are used by theadversary to locate the hotspot in addition to thatadversary can know that whenever it receives packetsfrom sensor nodes whether it is fake or real the adversarycan conclude that there is a hotspot in the network.

3.3Hotspot based Realistic Adversary using data Collector (HRADC):

In our hotspot model, here is individual a solitary server,repairingaamount of queues in a repeated manner, which consumesremainedoriginate to be inappropriate for hotspot location based privacy preserving applications.When the input load remainsmoreover high or the limitnecessitiesof the request are relativelydifficult, the hotspot may chooseto schedule severaldata collectorthrough different appointment tables allocatedto each. When the quantity of data collector is amplified, the perfectis rehabilitated to a hotspot based realistic adversary using data collectorsystemor multi server asking model, the carefulinvestigation of whichis not available. Assuming self-determiningdata collector, symmetricsituationdisseminated data arrivals, independent and identicallydisseminated service times and walk times in addition no serverhotspot adversary, an estimatedappearance for the mean in the offingtime can be consequent. Thetotal regular amount of work inward to the hotspot based realistic adversary using data collector per componentquantity of time.

Where

DC- Data collector,

H- Hotspot, N-Nodes in network,

L- Location

$$DC_s = \frac{H\lambda N[X]}{L}$$

The periodwait between two successive arrivals of any oneMC at a tagged device buffer q container be evaluated as

$$N[DC] = \frac{RA}{L - H\lambda N[X]}$$

ForLocation L = 1...n,

Sinceconstancy is certain by the finiteness of averagesequence time, to ensure constancy, the quantity of hotspot

$$L > H\lambda N[X]$$

In other words, the incoming data collector time

$$\lambda < \frac{L}{HN[X]}$$

Towardschange to the mean communication waiting time in the severalDC case, the appearance for mean waiting time in singlehotspot

$$\frac{N[X]}{L}, \frac{N[X^2]}{L^2}, \frac{N[W]}{[L(L-1)DC_S]}, \qquad then \frac{N[W^2]}{[L-(L-1)DC_S]}$$

Inrespectively,$E[X], E[X^2], E[W]\ and\ E[W^2]$thus,the mean waiting period in the manifoldof hotspot adversary in situation becomes data collector

$$DC_S = \frac{H[\frac{\lambda N[X^2]}{L} + \frac{N[W][L-\lambda N[X])}{L-(L-1)dc}]}{2(L - H\lambda N[X])}$$

Similar toward the undeveloped single HRADC network, here similarly, the probablewaiting time of the container in the sensor barrier and theregular sensor buffer residenceescalation with the packetarrival rateλ, number of sensors H and the dimensions of thedistribution area and condenses with the speed of HRADC. However,in cooperation performance metrics reduction with the amount of HRADC, thus manufacture the model improved suited for substantial inputload situations, memory-limited sensors, and then delay-sensitiveapplications. While the delay and distributionpresentation areenhanced by the use of several data collectors, energyconsumption and network generation are not affected, since theamount of transmissions and the variety of transmission arenot changed through the use of more quantity of HRADC. Takinginto interpretation the higher cost of HRADCassociated to ordinarysensor nodes, smallest number of HRADC that content theapplication-specific inexpressionrestrictions may be used.

IV. RESULT AND DISCUSSION:

The experimentations were approvedobtainablewith NS-2 as theimitation tool NS-2 is a separate event network emulatorwhich delivers a detailed perfect of the physical and linklayer performance of a wireless network. The situation is setup in a topology of 3000 m X 3000 m area, where 100nodes are casually deployed.The nodes radiobroadcast radius is 50m, then the monitoring devices'overhearing radius is ε, x50 m. The network consumes onehotspot that is casually located and immovable during eachimitation run, and the

amount of source nodes in thehotspot is 35. The quantity of monitoring strategies is Nm.The false optimistic probabilityis the likelihood that the adversary incorrectly identifies anarea as a hotspot. It is slow by the number of periodsthe adversary incorrectlyclassifies an area as a hotspot to thetotal amount of times the challenger suspects that an area isa hotspot. The reduction of the discoverylikelihood andthe increase of the false optimistic probability are indicatorsfor provided that high-privacy defense for the hotspot.In our scheme, the controlling adversary who consumes a largeamount of monitoring devices with large eavesdroppingradius will not find hotspots. We found that in the runsthat the adversary possibly will be close to the network, they could notaccomplish information about the site or the direction ofthe hotspot in the network.

Scheme	Nano Mins	5			10		
	Rounds	1	2	3	4	5	6
SLPPS		0	0.043	0.1	0.05	0.13	0.21
LAR-MPRA		0.023	0.075	0.058	0.18	0.33	0.46
Proposed scheme (HRADC)		0.045	0.1	0.23	0.34	0.62	0.72

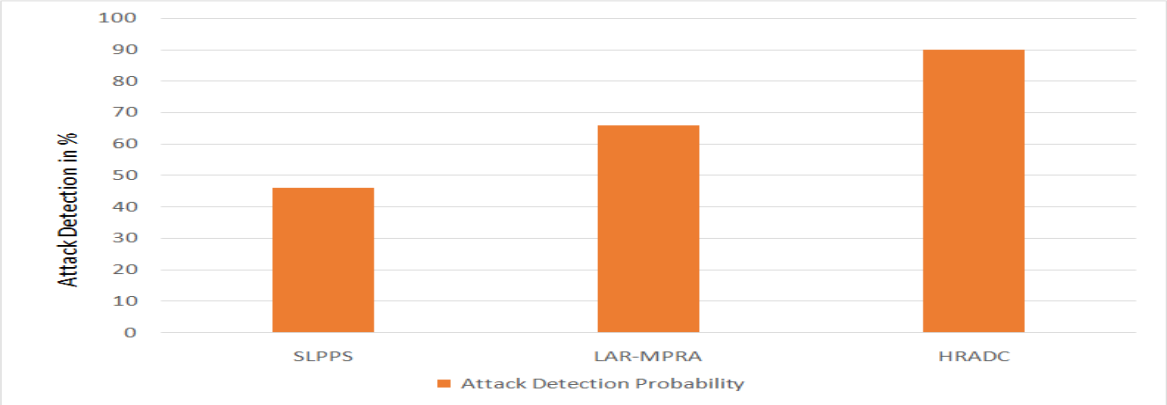
Table 4. 1. HRADC Based Detection probability

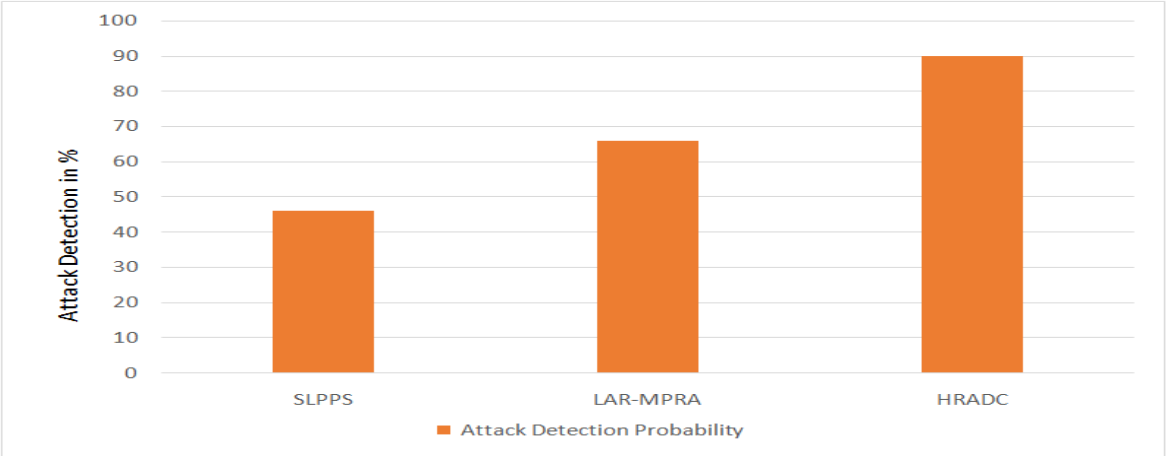
The simulation results assumed in Tables 4. 1 validatethat the no of attack detection and thediscovery possibility, when the throughput is increase timing.

The detection probability isthe prospect that the adversary can find the hotspotthroughout the simulation time. It is restrained by the number oftimes the adversary possibly will locate the hotspot to the totalnumber of runs. The false positive probability is thepossibility that the adversary falsely recognizes an area asa hotspot. It is measured by the quantity of times theadversary falsely recognizes an area as a hotspot to the totalnumber of times the adversary suspects that an expanse is a hotspot. The reduction of the detection likelihood and thegrowth of the false positive likelihood are indicators forprovided that high-privacy defense for the hotspot.

4.1 Attack Detection performance in network:

The detection probability isthe prospect that the adversary can find the hotspot attack detection in the simulation time. It is restrained by the number oftimes the adversary possibly will locate the hotspot to the totalnumber of runs.





The attack probability is theoption that the adversary falsely recognizes an area asa hotspot. It is measured by the quantity of times theadversary attack recognizes an area as a hotspot to the totalnumber of times the adversary suspects that an expanse is a hotspot. The reduction of the detection likelihood and thegrowth of the false positive likelihood are indicators forprovided that high-privacy defense for the hotspot.

4.2Energy consumption based on HRADC:

The energy point on the network is necessity and maximum important one of the speedy data message on their network. Its intended on or after their each node energy operation is necessity of the network. if some nodule none to data communicate with the meaning of node to placed aside the energy on the network.

Energy consumption = no of packets * initial energy level

Remained energy = energy consumption – no of packets in node

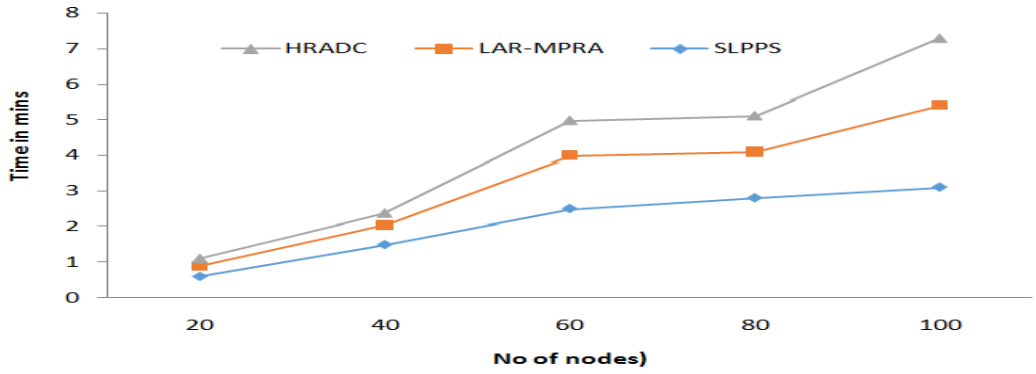


Fig 4.2. Energy level on network

Since themchoice the node through the higher remaining energy in the collection as the hotspot for the next round. However, this organizes not assure the determinedcontinuation of the overall network lifetime. Therefore, if the node through the maximum residual liveliness is a node located at the side of the data collector, this can lead other nodes to occupysubstantialquantities of energy to spread that node, which cannot be energy effectual for the entire network.

4.3Throughput Performance in network:

This metric provides an estimation of how competent a sending protocol is, in the meantime the number of routing packets sent per data packet gives an idea of just how well the procedure keeps the sending in order efficient. The higher the standardsendingload metric is, the higher the directly above of routing packets and subsequently the lower the efficiency of the protocol. This is the output of total number of customary data packets divided by total number of sent data packets.

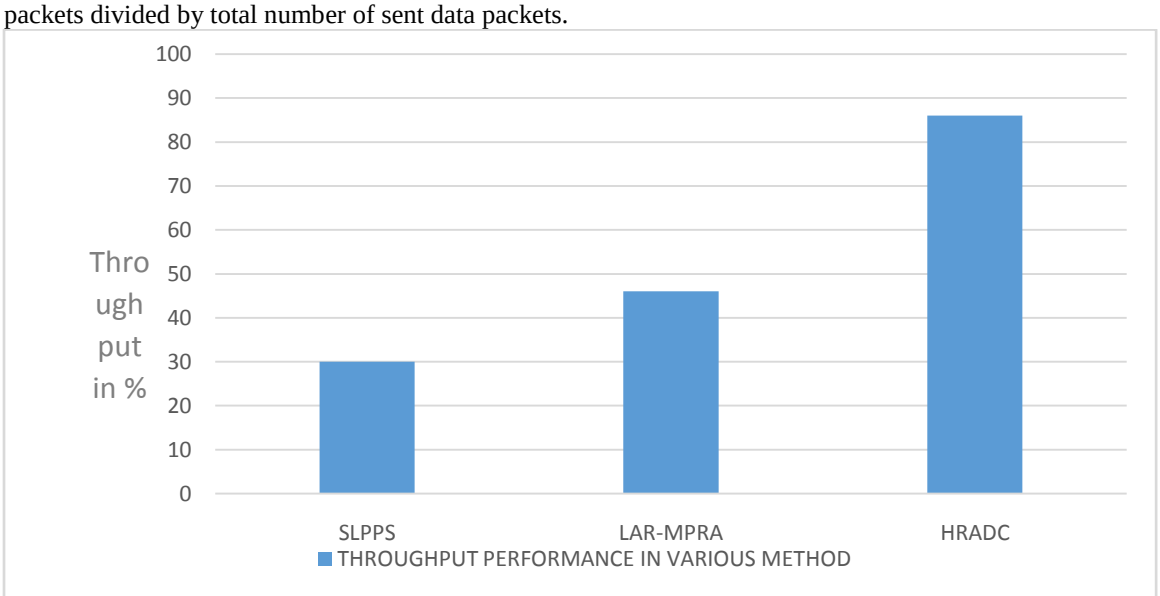


Fig 4.3. Throughputlevel on network

V. CONCLUSION:

In this paper, by means of realistic adversary model we consumepresented a context aware location privacy, and we alsoplanned a sink node for protective the location of thehotspot by creating road traffic of fake containers and sendingpackets completedissimilar routes in addition packets arrival isaltered at each hop.A source position privacy-preserving that makes a storage of fake packet around the source node, in differs traffic ways and variations the packets arrival at each hop. We discussed then concluded that smooth if the opponent model does not have a global opinion to the network circulation, so we can find a hotspots by means of some few intensive care devices and by means of simple traffic examination techniques. Our scheme can deliver a strong defense against Hot-spot Locating attack through much less liveliness cost associating to global-adversary-based schemes.

REFERENCES

[1]. S. Saravanan and M. Prabakaran, "Enhanced Privacy Preserved Secure Data Transfer Using MPRA-LAR Routing in Wireless Sensor Networks", July 2015
[2]. Basavarajeshwari, M. Jitendranath, Manimozhi, "Mitigating Hotspot Locating Attack in WirelessSensor Network" June 2013
[3]. Liam Murphy, "Planning Base Station and Relay Station Locations for IEEE 802.16j Network with Capacity Constraints". July 2011
[4]. Nabil H. Mustafa, "PTAS for Geometric Hitting Set Problems via Local Search" June 8–10, 2009
[5]. Yan Chen, Shunqing Zhang, ShugongXu, and Geoffrey Ye Li, "Fundamental Tradeoffs on Green Wireless Networks", January 25, 2011.
[6]. HaiyingShen, Member, IEEE, and Lianyu Zhao, Student Member, IEEE "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" , June 2013
[7]. J. Deng, R. Han, and S. Mishra, "Countermeasuresagainst Traffic Analysis Attacks in Wireless SensorNetworks," Sept. 2005.
[8]. H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," Computer Networks, July, 2009.
[9]. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk,"Enhancing Source Location Privacy in SensorNetwork Routing, June2005.
[10]. X. Cheng, A. Thaeler, G. Xue, and D. Chen, "TPS: A Time-Based Positioning Scheme for Outdoor Wireless Sensor Networks," Mar. 2004.