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

1S. Saravanan, 2Dr. M. Prabakaran
1Research Scholar, Assistant Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamilnadu, India.
2Research 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 the network and can analyze the traffic in those areas. Next we propose an attack based privacy preserving scheme by creating fake traffic of irregular shape which provides an efficient mechanism to protect the source node's location in addition to that we also generate the fake packet at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network. Next we are introducing the concept of context aware location privacy where the sensor nodes are having the 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.

INTRODUCTION

Wireless sensor network contain of insignificant, multifunctional and reserve forced sensors. Every time sensor node identifies something it may be fighter in military request and common physical in case of environment monitoring it intelligent that event to the sink which is a commanding data collection unit. In this paper we consider environment monitoring request where the devices are used to monitor the nodes, for instance a WSN consume been organized to monitor the all foundation based location. The sensors infrequently sense the data of their occurrence and activities and the detected data is described to the sink. However, WSN are positioned in large and open areas so that providing corporal boundary or appearing each sensor node grow into almost impossible.

While the info is sent from foundation to the sink finished the broadcast link, the adversaries can eavesdrop on the wireless medium and container locate the source nodes by creation use of traffic gen to the network. Therefore it is important to preserve the foundation node's location because of the acceptance of locating hotspot and their fur's big market value. In the international adversary founded scheme the adversary has the competence to monitor the each radio transmission and the links among them. In this structure it is it is expected that adversary can monitor the complete network which is impracticable in large areas.

Adversary is having international view of the network incomes that the assailant can locate node without the use of network transmissions. Wedetermination study the hot spot occurrence in which challenger tries to discover the hotspot by analyzing the traffic evidence collected by the intensive care devices. Adversary follows the traffic investigation techniques such as time associations, packet relationships and nodes sending rates to find the hotspot. Finally we propose our hotspot based context aware scheme in which we make a detection of fake traffic in adding to that we also make the fake event at a specific time interval so that opponent cannot associate the expected hotspot regions similar sink node with the variations in the network to break the incompatibility in the traffic pattern produced by hotspot to complicate the source node inside the collection of nodes.
Hereto decrease the energy consumption of conducting nodes we 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 are directed in a more well-organized and confidentiality preserving manner. The solution aims to expect the actions of the attacker in instruction to reduce the number of packets is able to detention and analyses, hence dropping the likelihood of 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 busses 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 the proposed method, privacy and preservation methods are enhanced. The secured logging contains six major functionalities 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 deals with sensitive information not displaying during search.

Data logs deals with the data history for identifying appropriate users. Privacy scheme deals with file linking and data access history. Preservation deals with enhanced 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 a wide number of areas such as commerce, emergency services, military, education, and entertainment. The network can leak confidential 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 to detect or more damaging than accidental ones: external adversaries may penetrate the data storage provider, or employees of the service provider may commit an insider attack [6, 7]. These concerns have prevented security conscious enterprises 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 roof sensor nodes organized in the intensive care area which are having the aptitudes to detect a hotspot. The source node and sink are stationary. The sensor nodes have incomplete battery power, addition capacity and limited network announcement bandwidth. Each sensor node is equipped with sensing device, data processing and interactive components. The sink has enough computation and storing capabilities to achieve the functions:

1) Broadcasting beacon packets to bootstrap our scheme.
2) Collecting the data sensed by the sensor nodes.

Hotspot have surrounded radio incidence tags and as soon as sensor node senses a hotspot, the node is called source node which refers event packet to the sink.

3.1 Attack discovery-Based Scheme for Adversary Model:

An attack 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.

3.2 Context Aware Location Privacy based Hotspot Locating:

A Context Aware Location Privacy is produced, when after small area large statisticsof packages are sent since sensor node which causesindiscretion in the linkage so that enemy makes use of these 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 the adversary to locate the hotspot in addition to that adversary can know that whenever it receives packets from sensor nodes whether it is fake or real the adversary can conclude that there is a hotspot in the network.

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

In our hotspot model, here is individual a solitary server, repairing a amount of queues in a repeated manner, which consumes remained origin to be inappropriate for hotspot location based privacy preserving applications. When the input load remains moreover high or the limit necessities of the request are relatively difficult, the hotspot may choose to schedule several data collector through different appointment tables allocated to each. When the quantity of data collector is amplified, the perfect is rehabilitated to a hotspot based realistic adversary using data collector system or multi server asking model, the careful investigation of which is not available. Assuming self-determining data collector, symmetric situation disseminated data arrivals, independent and identically disseminated service times and walk times in addition no server hotspot adversary, an estimated appearance for the mean in the offing time can be consequent. The total regular amount of work inward to the hotspot based realistic adversary using data collector per component quantity of time.

Where

- DC - Data collector,
- H - Hotspot, N - Nodes in network,
- L - Location

\[ DC_s = \frac{HAN[X]}{L} \]

The period wait between two successive arrivals of any one MC at a tagged device buffer q container can be evaluated as

\[ N[DC] = \frac{RA}{L - HAN[X]} \]

For Location \( L = 1 \ldots n \), since constancy is certain by the finiteness of average sequence time, to ensure constancy, the quantity of hotspot \( L > HAN[X] \)

In other words, the incoming data collector time

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

Towards change to the mean communication waiting time in the several DC case, the appearance for mean waiting time in single hotspot

\[ \frac{N[X]}{L}, \frac{N[X^2]}{L^2}, \frac{N[W]}{L(L - 1)DC_s}, \text{ then } \frac{N[W^2]}{L - (L - 1)DC_s} \]

In irrespectively, \( E[X], E[X^2], E[W] \) and \( E[W^2] \) thus, the mean waiting period in the manifold of hotspot adversary in situation becomes data collector

\[ DC_s = \frac{H[\frac{2N[X]}{L} + \frac{N[W][L - 2N[X]]}{L - (L - 1)DC_s}]}{2(L - HAN[X])} \]

Similar toward the undeveloped single HRADC network, here similarly, the probable waiting time of the container in the sensor barrier and the regular sensor buffer residence escalation with the packet arrival rate \( \lambda \), number of sensors \( H \) and the dimensions of the distribution area and condenses the speed of HRADC. However, in cooperation performance metrics reduction with the amount of HRADC, thus manufacture the model improved suited for substantial input load situations, memory-limited sensors, and then delay sensitive applications. While the delay and distribution presentation are enhanced by the use of several data collectors, energy consumption and network generation are not affected, since the amount of transmissions and the variety of transmission are not changed through the use of more quantity of HRADC. Taking into interpretation the higher cost of HRADC as associated to ordinary sensor nodes, smallest number of HRADC that content the application-specific in expression restrictions may be used.

IV. RESULT AND DISCUSSION:

The experimentations were approved obtainable with NS-2 as the imitation tool NS-2 is a separate event network emulator which delivers a detailed perfect of the physical and link layer performance of a wireless network. The situation is setup in a topology of 3000 m x 3000 m area, where 100 nodes are casually deployed. The nodes radiobroadcast radius is 50 m, then the monitoring devices' overhearing radius is \( \epsilon \times 50 \) m. The network consumes one hotspot that is casually located and immovable during each imitator run, and the
amount of source nodes in the hotspot is 35. The quantity of monitoring strategies is $N_m$. The false optimistic probability is the likelihood that the adversary incorrectly identifies an area as a hotspot. It is slow by the number of periods the adversary incorrectly classifies an area as a hotspot to the total amount of times the challenger suspects that an area is a hotspot. The reduction of the discovery likelihood and the increase of the false optimistic probability are indicators for provided that high-privacy defense for the hotspot. In our scheme, the controlling adversary who consumes a large amount of monitoring devices with large eavesdropping radius will not find hotspots. We found that in the run that the adversary possibly will be close to the network, they could not accomplish information about the site or the direction of the hotspot in the network.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Nano Mins</th>
<th>5</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rounds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLPPS</td>
<td>0</td>
<td>0.043</td>
<td>0.1</td>
</tr>
<tr>
<td>LAR-MPRA</td>
<td>0.023</td>
<td>0.075</td>
<td>0.058</td>
</tr>
<tr>
<td>Proposed scheme (HRADC)</td>
<td>0.045</td>
<td>0.1</td>
<td>0.23</td>
</tr>
</tbody>
</table>

Table 4.1: HRADC Based Detection probability

The simulation results assumed in Tables 4.1 validate that the no of attack detection and the discovery possibility, when the throughput is increase timing.

The detection probability is the prospect that the adversary can find the hotspot throughout the simulation time. It is restrained by the number of times the adversary possibly will locate the hotspot to the total number of runs. The false positive probability is the possibility that the adversary falsely recognizes an area as a hotspot. It is measured by the quantity of times the adversary falsely recognizes an area as a hotspot to the total number of times the adversary suspects that an expanse is a hotspot. The reduction of the detection likelihood and the growth of the false positive likelihood are indicators for provided that high-privacy defense for the hotspot.

4.1 Attack Detection performance in network:
The detection probability is the prospect that the adversary can find the hotspot attack detection in the simulation time. It is restrained by the number of times the adversary possibly will locate the hotspot to the total number of runs.
The attack probability is the option that the adversary falsely recognizes an area as a hotspot. It is measured by the quantity of times the adversary attack recognizes an area as a hotspot to the total number of times the adversary suspects that an expanse is a hotspot. The reduction of the detection likelihood and the growth of the false positive likelihood are indicators for provided that high-privacy defense for the hotspot.

**4.2 Energy 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.

\[
\text{Energy consumption} = \text{no of packets} \times \text{initial energy level} \\
\text{Remained energy} = \text{energy consumption} - \text{no of packets in node}
\]

![Fig 4.2. Energy level on network](image)

Since the node through the higher remaining energy in the collection as the hotspot for the next round. However, this organizes not assure the determined continuation 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 occupy substantial quantities of energy to spread that node, which cannot be energy effective for the entire network.

**4.3 Throughput 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 standardsending load 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. Throughput level on network](image)
V. CONCLUSION:

In this paper, by means of realistic adversary model we consume presented a context aware location privacy, and we also planned a sink node for protective the location of the hotspot by creating road traffic of fake containers and sending packets completed dissimilar routes in addition packets arrival is altered 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

[3]. Liam Murphy, “Planning Base Station and Relay Station Locations for IEEE 802.16j Network with Capacity Constraints”. July 2011
[6]. Haiying Shen, Member, IEEE, and Lianyu Zhao, Student Member, IEEE “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”. June 2013