# Controlled Cloud-Based SaaS Service Scheme to Denial the Hotspot-Locating Attacks in Wireless Sensor Networks

K.Jegadeeswaran,
Assistant Professor(Sr.G)
Sri Ramakrishna Engineering College
Coimbatore,T amil Nadu,India
*jagadeeswar@gmail.com*

S.Ramakrishnan,
Assistant Professor
Sri Ramakrishna Engineering College
Coimbatore, Tamil Nadu, India
*ramakrishnan@srec.ac.in*

M.Mailsamy
Lecturer(Sr.G)
Sri Ramakrishna Polytechnic College
Coimbatore, Tamil Nadu,India
*myilsrisakthi@gmail.com*

***Abstract***—The wireless sensor networks opponent can make use of the traffic information's to locate the monitored objects in Software as a service(Saas) , e.g., to identify the opponent soldiers. In this paper, we first define a hotspot phenomenon through SaaS and it causes an obvious inconsistency in the network traffic pattern due to the large volume of packets originating from a small area in Partial controlled cloud based scheme. Second, we develop a realistic opponent model, assuming that the opponent can monitor the network traffic in multiple areas, rather than the entire network or only one area. Using this model, Hotspot-Locating where the opponent uses traffic analysis techniques to locate hotspots. Finally, we propose a controlled cloud-based SaaS scheme for efficiently protecting against Hotspot-Locating attack by creating a controlled cloud with an irregular shape of fake traffic, inconsistency in the traffic pattern and camouflage the source node in the nodes forming the controlled cloud. To reduce the energy cost, controlled clouds are active only during data transmission and the intersection of controlled clouds creates a larger merged controlled cloud, to reduce the number of fake packets and also boost preservation. Simulation and analytical results demonstrate that our scheme can provide stronger protection than routing-based schemes and requires much less energy than global-adversary schemes.

***Key Words***—*Wireless sensor network , source-location -preserving schemes, context , and anonymity ,merged controlled cloud.*

*****

## I. Introduction

A wireless sensor network (WSN) consists of a large number of sensing devices, called sensor nodes, which are interconnected through wireless links to perform distributed sensing tasks. WSN have found many useful applications for automatic data collecting , such as habitat monitoring, military surveillance, and target tracking, for monitoring the activities of enemy soldiers or valuable assets, e.g., endangered animals. When a sensor node detects a soldier or an endangered animal, it reports the event to the data collector called the Sink. This data transmission may occur via multi hop transmission, where the sensor nodes act as routers. In this paper, we consider habitat monitoring applications where the WSN is deployed for monitoring pandas. For example, a WSN has been deployed by the Save-The-Panda Organization to monitor pandas in a wild habitat While pandas move in the network, their presence and activities are periodically sensed by the sensor nodes and reported to the Sink. However, WSNs are usually deployed in open and large areas that are unattended and lack of protected physical boundary, which makes the networks vulnerable to many threats. Since the sensed data are typically transmitted through wireless channels, opponent can eavesdrop on the open and shared wireless medium and make use of traffic information to locate source nodes to hunt pandas.

The threats can usually be classified into: content and contextual . For the content threat, the opponent attempts to observe the content of the packets sent in the network to learn the sensed data and the identities and locations of the source nodes. This threat can be countered by encrypting the packets' contents and using pseudonyms instead of the real identities. For the contextual threat, the opponent eavesdrops on the network transmissions and uses traffic analysis techniques to deduce sensitive information, including whether, when, and where the data are collected. Actually, the act of packet transmission itself reveals information even if the packets are strongly encrypted and the opponent could not interpret them.

## II. RELATED WORKS

Recently, location in wireless and wired networks has gained much attention. Different schemes have been developed to protect users' in location tracking systems. Which determine the users' positions for location-based services. Location in these schemes is content oriented, where location information is collected and protected as the users' private data. An Onion routing provides the anonymous communications for the Internet by hiding the identities of the end users of a communication session. The proposed schemes in conceal the nodes' network/MAC addresses in order to achieve anonymous communications for mobile ad hoc networks. However, these schemes employ different network and threat models from the ones suitable for the source location problem in sensor networks

Routing-based schemes preserve source nodes' location by sending packets through different routes to make back tracing the movement of the packets from the Sink to the source nodes infeasible. In a random-walk-based -preserving scheme, called Phantom, is proposed. Each packet takes a random walk to a random location before . it is sent to the Sink. However, the scheme fails if the opponent's overhearing range is more than the sensor nodes' transmission range.

Global-opponent-based schemes assume that opponent can monitor the traffic of the entire network. Each node has to periodically send packets, and send dummy packets if it does not have sensed data so that it is infeasible for the opponent to distinguish between the real and dummy packets.

# III. NETWORK AND OPPONENT MODELS

## 3.1 Network Realistic Model

As illustrated in Fig. 1, the considered WSN consists of the Sink and a large number of homogeneous panda-detection sensor nodes which are randomly deployed in an area of interest. The Sink and the sensor nodes are stationary. The sensor nodes are resource-constrained devices with low battery.

power and computation capacity, but equipped with sensing, data processing, and communicating components.

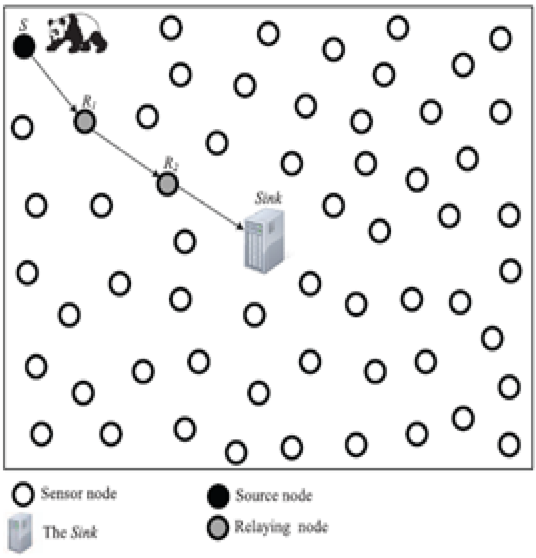

**Fig. 3 The Architecture of considered WSN**

## 3.2 Opponent Based Model

The opponent is a hunter who eavesdrops on the wireless transmissions and attempts to make use of the network traffic to determine the locations of pandas to hunt them. The opponent distributes a group of monitoring devices in areas of interest, called observation points, to collect the traffic information in these areas, but he cannot monitor the traffic of the entire network.

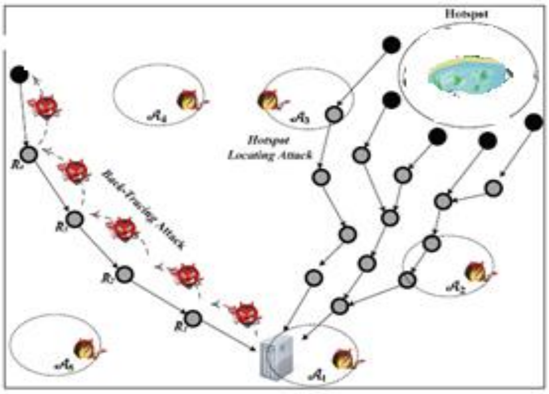

**Fig.2. The Opponent Model**

# IV. HOTSPOT-LOCATING ATTACK

## 4.1 Hotspot Phenomenon for WSN

A hotspot is formed when a large volume of packets are sent from the sensor nodes of a small area, causing an obvious inconsistency in the network traffic which may last for some time. The opponent attempts to make use of this traffic inconsistency to locate hotspots to hunt pandas. Figs. 3 and 4 can illustrate the hotspot phenomenon. Fig. 3 shows the average packet sending rate of each sensor node when there are no hotspots and using the shortest path routing scheme. In this scheme, the nodes send the sensed data to the Sink through the minimum number of relaying nodes. This traffic pattern is obtained when the number of pandas sensed by each sensor node and the time spent by pandas at each node

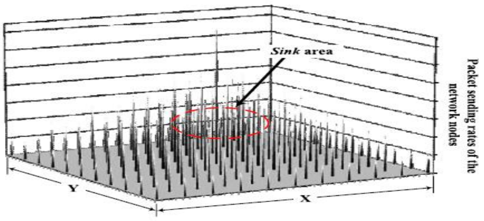

**Fig. 3 The packet sending rate of each node without hotspots.**

## 4.2 Hotspot-Locating Attack

Fig. 5 shows the flowchart of a Hotspot-Locating attack using the opponent model discussed in Section 3.2. In the initial phase, the opponent deploys a monitoring device near of the Sink and deploys the other devices at initial observation points distributed in the network are uniformly distributed. It can be seen that the nodes near the Sink send a significantly larger volume of packets than the nodes further away, and the packet sending rates gradually decrease aswemove to the network edges .

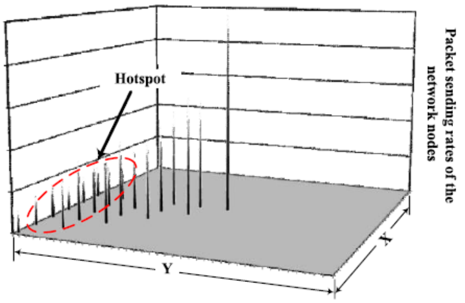

Fig. 4. The packet sending rate of each node with a hotspot.

## V. CONTROLLED CLOUD-BASED SAAS SCHEME

### 5.1 Predeployment Phase

Before deploying the network, each sensor node A is loaded with a unique identity IDA, a shared key with the Sink KA, and a secret key dA that is used to compute a shared key with any sensor node using identity-based cryptography (IBC) based on bilinear pairing.

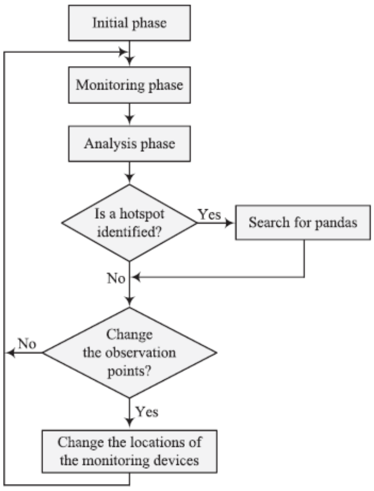

Fig. 5. The flowchart of *Hotspot-Locating* attack.

### 5.2 Bootstrapping Phase

This phase is performed only one time in the lifetime of the network, after the network is deployed and before it starts data collection. This phase has three main purposes:1) informing the Sink about the nodes' locations to link an event to its location; 2) assigning fake source nodes and discovering the shortest routes to the Sink; and 3) forming groups that are used in creating controlled clouds. After deploying the network, the Sink broadcasts a beacon packet and each sensor node adds its identity and broadcasts the packet. Each node can know the shortest route to the Sink which includes the identities of the nodes in the first received beacon packet. Every sensor node determines its own location information using some localization methods such as those proposed in  and notifies the Sink through the shortest route.

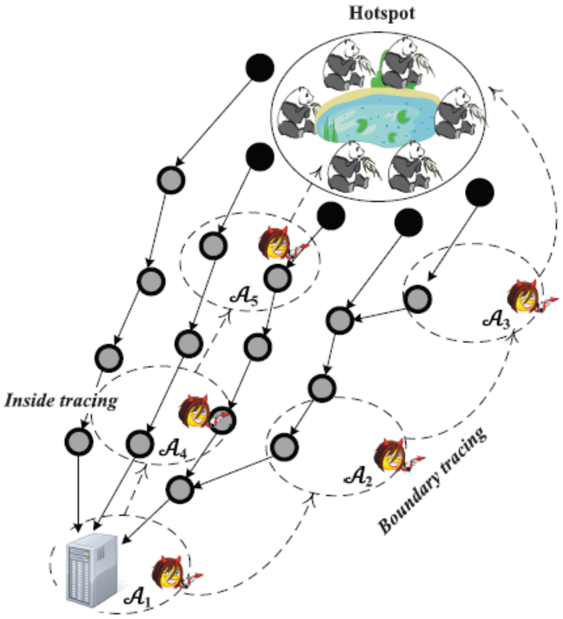

**Fig. 6.Inside and boundary back tracing for locating hotspots.**

In order to assign fake source nodes, node A broadcasts Fake Nodes Request Packet (FREQ) that contains the maximum number of hops (hmax) the packet can be propagated. Each node adds its identity and broadcasts the packet if the number of hops is fewer than hmax; otherwise, it unicasts Fake Nodes Request Reply (FREP) packet to node A, containing the identities of the nodes in the route. Node A receives multiple FREP packets containing different routes with maximum number of hops of hmax. It chooses a group of

nodes at different number of hops and unicasts the Fake Node Assignment Packets (FASS) to assign them as fake source nodes to its packets. For each FASS packet, node A adds the identities of the nodes in the route and a random value that will be used to generate pseudonyms shared between each two neighboring nodes in the route.

### 5.3 Event Transmission Phase

is the guarantee that information in its general sense is observable or decipherable by only those who are intentionally meant to observe or decipher it. According to Pfitzmann and Kohntopp anonymity is defined as the state of being unidentifiable within a set of objects called the anonymity set.

The essence of our scheme is based on the principle that one of the best ways to avoid being identified is to mix with the crowd. Our scheme conceals a source node within a group of nodes with an irregular shape, called “controlled cloud.” A source node is considered to have a complete anonymity if the opponent cannot identify it in the controlled cloud, i.e., the opponent may be able to know that a node in a controlled cloud sends an event packet, but he cannot identify this node.

## VI. EVALUATIONS

### 6.1.1 Analysis

For Pseudonyms unlink ability, the opponent cannot link the pseudonyms of one sequence. The importance of thisproperty lies in the fact that if an opponent could link a pseudonym to a node, he will not benefit from this conclusion in the future. In our scheme, generating or correlating pseudonyms is infeasible without knowing the secret key used in generating them. Even if there is only one transmission, fake packets can make pseudonyms linkability infeasible because the opponent cannot distinguish between event and fake packets. Pseudonym collision means that more than one node have the same pseudonym, because the hash function may generate the same hash value from hashing two different inputs.

For packet length correlation, the packets of one flow can be correlated if they are distinguishable from their lengths. To prevent this, all packets should have the same length, or random length by adding random-length padding bits at each relaying node. For packet sending time correlation, an opponent tries to deduce the forwarding path by observing the transmission time of a node and its neighbours. The opponent makes use of the fact that the nodes usually relay packets after short delay and based on first-received-first transmitted basis. Changing packets’ appearance at each hop cannot prevent this correlation because it depends on the packets’ sending times and not the content. To obfuscate the temporal relationship between the transmissions of consecutive

For fake and real source nodes unlink ability, if an opponent could locate a fake source node, he should not gain any information about the location of the corresponding real source node. This link ability is infeasible because each real source node sends its packets through multiple fake sources, each fake source node serves different real sources, and the distance between a fake source node and the real source is random. If the distance between a fake source Fig. 11. Merging controlled clouds. node and the real one is fixed or has a minimum number of hops (dmin), the opponent can figure out the relative location of the real source node or conclude that it cannot be in the fake source node’s dmin-hop neighbours. What also makes this link ability infeasible is that the opponent observes all the transmissions of a controlled cloud random because he cannot distinguish between fake and real packets. For controlled cloud shape and source node unlink ability, if a strong opponent could trace a part of a controlled cloud or all the controlled cloud, he cannot infer any information about the source node’s location. For example, if a controlled cloud is circle shaped and the source node is located at the centre, the opponent can gain some information about the source node’s location by tracing a part of the controlled cloud. In our scheme, this link ability is infeasible because controlled clouds are irregular and changeable, and some nodes may belong to multiple controlled clouds at the same time, which creates an overlapped and complex merged controlled cloud.

For merged-controlled cloud splitting attack, the opponent tries to reduce the size of a merged controlled cloud, e.g., to reduce the anonymity set. In our scheme, the traffic of individual controlled clouds is indistinguishable because a controlled cloud’s packets do not have any data that refer to the controlled cloud, and thus the opponent cannot split a merged controlled cloud or even identify the boundaries of the individual controlled clouds. Controlled cloud merging can increase the anonymity set without extra overhead, e.g., if two controlled clouds each with nc nodes are merged, the anonymity sets of the individual controlled clouds are nc but the anonymity set of the merged controlled cloud is 2nc_no, where no is the number of nodes belonging to the two controlled clouds.

For packet back tracing attack, it is unlikely that the opponent will continuously receive event packets from a source node because packets are sent through different fake source nodes which can be far from each other. What also complicates this attack is that event packets sent from a real or fake source node at different times are uncorrelated. Moreover, even if the opponent could capture the same packet at different relaying nodes, he cannot correlate the packets. Even if the opponent could trace back packets to a fake source node, he cannot locate the corresponding real source node due to the fake and real source nodes unlink ability.

For packet-replay attack, the opponent tries to replay old packets repeatedly in order to observe the traffic patterns of packet forwarding, e.g., to figure out the network topology to locate source nodes. This is infeasible because the opponent cannot compute fresh pseudonyms and the nodes drop packets if they cannot recognize their pseudonyms. For packet sending rate analysis, the opponent attempts to make can still analyses the packet sending rate. Our scheme uses fake packets to camouflage the nodes that are close to pandas with the other nodes in the controlled cloud in such a way that makes this spot indistinguishable.

For event packets flow recognition attack, the opponent attempts to recognize the flow of real packets to identify the source node or at least a small area around it. For example, from Fig. 8, if the opponent could recognize the flow of the real packets from node B to F, he can deduce that the panda cannot be in the region between B and F and reduce theanonymity set. In our scheme, the event and the fake packets are indistinguishable and the opponent cannot correlate an event packet as it is relayed from the real source node to the fake one.

Event un observability means that the opponent cannot know whether pandas are sensed or not. However, this property is not important in habitat monitoring application especially when the network is large and exhaustive search for pandas is infeasible.

Routing-based -preserving schemes use metric called safety period which is the number of packets the opponent has to capture in order to move from the Sink to a source node. Stronger protection can be achieved with increasing the safety period. This metric is not accurate because it measures the best case when the opponent starts from the Sink, but if the opponent captures a packet at any relaying node, the safety period decreases.

### 6.1.2 Simulation Results

We have built up a discrete and event-based simulator to evaluate the effectiveness of the Hotspot-Locating attack and the protection of our scheme and routing-based schemes. Four thousand nodes are uniformly randomly .

**TABLE 1**

**Simulation Parameters**

| Parameter | Value |
|---|---|
| Number of nodes | 300 |
| Network size | 3500m*3500m |
| Number of hotspot | 1 |
| Number of sensor nodes in hotspot | 5 |
| A sensor node`s transmission range | 50m |
| Opponent`s hearing range | E * 50 m |
| Sink Location | Center |
| Sensor nodes and the hotspot | Uniformly distributed |
| Event transmission rate | 1/30 seconds |

**TABLE 2**

**False Positive Probability**

| Scheme | N | 4 | | | 8 | | |
|---|---|---|---|---|---|---|---|
| | E | 1 | 2 | 4 | 1 | 2 | 4 |
| Shortest Path | | 0.2 | 0.1 | 0.1 | 0.1 | 0.1 | 0 |
| My Scheme | | 1 | 0.8 | 0.9 | 0.8 | 0.9 | 0.8 |

**TABLE 3**

**Hotspot Detection Probability**

| Scheme | N | 4 | | | 8 | | |
|---|---|---|---|---|---|---|---|
| | E | 1 | 2 | 4 | 1 | 2 | 4 |
| Shortest Path | | 0.7 | 0.7 | 0.9 | 0.8 | 0.9 | 1 |
| My Scheme | | 0 | 0.5 | 0.7 | 0.5 | 0.7 | 0.2 |

The simulation results given in Tables 2 and 3 demonstrate that the false positive probability decreases and the detection probability increases when the monitoring devices overhearing radius increases. This is because the opponent can monitor more nodes and collect more accurate traffic information.This is because the shortest-path scheme does not preserve location and the Phantom scheme cannot prevent packet correlation and conceal traffic analysis information. The slight improvement in the location protection with increasing hw is because of adding little randomness to the network traffic.

In our scheme, the powerful opponent who has a large number of monitoring devices with large overhearing radius will not locate hotspots. We found that in the runs that the opponent could be close to the controlled cloud, he could not conclude information about the location or the direction of the hotspot in the controlled cloud. The few times the opponent could locate the hotspot were random. Therefore, what an opponent can do is to exhaustively search the controlled cloud.

### 6.2 Energy Cost

When using cryptosystems is necessary to prevent packet correlation, and using fake packets can boost source nodes' location preservation. To reduce the energy cost, our scheme uses energy efficient cryptosystems, including hash function and symmetric key cryptography, and avoids the extensively energy consuming asymmetric-key cryptography. From gives the consumed energy for sending/ receiving 1 bit and computing the cryptographic operations required for our scheme. We can see that the hashing and symmetric-key encryption/decryption operations consume low energy comparing to pairing operations.Since the Sink has more computational and energy capabilities than the sensor nodes, the nodes in the route

Comparing to global-opponent-based schemes, our scheme uses fake packets much more efficiently by sending them only if there is an event instead of periodically. Moreover, fake packets are sent only in the active controlled cloud instead of flooding the entire network, and controlled cloud merging can reduce the number of fake packets. Although our scheme requires more cryptographic operations than global-opponent-based schemes, these operations consume much less energy than transmitting/receiving packets, as indicated in Table 3. the required energy for transmitting 1 KB of data over 100 m consumes as much energy as executing three million microprocessor instructions.

## VII. CONCLUSION AND FUTURE WORK

In this paper, we have introduced a novel attack to locate source nodes in WSNs, called Hotspot-Locating, which uses a realistic opponent model using the Software as a Services. We have also proposed a source location -preserving scheme that creates a controlled cloud of fake packets around the source node, varies traffic routes, and changes the packets' appearance at each hop. We have shown that even if the opponent does not have a global view to the network traffic, he can locate hotspots using few monitoring devices and simple traffic analysis techniques. Our simulation and analytical results have demonstrated that routing-based schemes cannot preserve the location of hotspots because they cannot conceal the traffic-analysis information. Moreover, our scheme can provide a strong protection against Hotspot-Locating attack with much less energy cost comparing to global-opponent-based schemes. In our future work, we will try sophisticated approaches to implement the IASS locate hotspots with low false-positive probability. In other words, we will use these algorithms to locate hotspots in the traffic-pattern image created by the traffic analysis techniques.

## REFERENCES

[1] Protecting Source Location Privacy against Hot-Spot Locating Attacks in Wireless Sensor Networks using Partial Controlled cloud-Based Scheme S.Ramakrishnan, R.Velmani, N.Sakthivel International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 .

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

[3] A. Arora et al., "A Line in the Sand: A Wireless Sensor Networkfor Target Detection, Classification, and Tracking," ComputerNetworks, vol. 46, pp. 605-634, 2004.

[4] "WWWF-the Conservation Organization," http://www.panda.org/, 2012.

[5] Star News, Panda Poaching Gang Arrested, Shanghai StarTelegram, Apr. 2003.

[6] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "EnhancingSource Location in Sensor Network Routing," Proc. IEEEInt'l Conf. Distributed Computing Systems (ICDCS '05), pp. 599-608,June 2005.

[7] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "TowardsEvent Source Unobservability with Minimum Network Traffic inSensor Networks," Proc. First ACM Conf. Wireless Network Security(WiSec '08), pp. 77-88, Apr. 2008.

[8] K. Pongaliur and L. Xiao, "Maintaining Source UnderEavesdropping and Node Compromise Attacks," Proc. IEEEINFOCOM, Apr. 2011.

[9] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient -Preserving Scheme against Traffic Analysis Attacks in NetworkCoding," Proc. IEEE INFOCOM '09, Apr. 2009.