

# FACILITATE SCHEME FOR DETECTING HOTSPOT INCURSION IN WIRELESS SENSOR NETWORKS

**P.SASIKALA,**

*Research Scholar, Department of Computer Science,  
Vivekanandha College of Arts and Sciences for Women,  
Tiruchengode-637205.*

**Miss M.P.SUBASHINI, (Guide),**

*Assistant Professor, Department of Computer  
Application, Vivekanandha College of Arts and Sciences  
for Women, Tiruchengode-637205.*

## ABSTRACT

*Wireless sensor network provides unauthorized person to make use of traffic information located on the monitoring of the objects. In this paper presenting of the hotspot incident that causes an obscure apparent to inconsistency in the network traffic prototype due to the large volume of packets originating from a small area. We are developing a practical foe model assume that the challenging can be monitoring of the network traffic in multiple areas quite then the entire network only one location. We introduce a novel attack call the hotspot incursion where the foe uses to traffic analysis techniques to locate hotspots. The proposed a facilitate scheme for efficiently defensive source node's area privacy beside Hotspot- Location Incursion by developing a fog with an uneven shapes of fake to the traffic detain the inconsistency the traffic pattern and legerdemain the source node in the node forming the fog. To reduce the vigor cost fog activities only during data transmission and the junction of the fogs with a largest complex fog to decrease the number of fake packets and also rise privacy safeguarding.*

**Index Term- Wireless Sensor Network, Hotspot, Privacy-Preserving Location Monitoring, Back Tracing Attacks.**

## 1. INTRODUCTION

Wireless sensor networks refers to an assorted system consisting of numerous recognition stations called sensor nodes with a infrastructure transportation wished-for to watch and document circumstances at miscellaneous locations [3]. Also sensor networks are answerable for sensing and communication of data. Since large quantity of data is to be processed with incomplete number of sensor nodes, data communication is dangerous and testing task becomes difficult [2]. Hence routing protocols for such kind of networks should be premeditated by bearing in

mind about these restrictions. In the conservative wireless networks, the node energy is predetermined and cannot be charged, hence ability to use energy inefficiently is a major factor to be well thought-out for routing protocol. To huge measure of sensor nodes, recharging the batteries in WSNs are infeasible task [1]. Hence, network natural life is a most important concern in sensor network drawing. In order to regulate and to make longer the network lifetime, several routing protocols exists. These routing protocols are confidential into two types depending on network topology: Unexciting direction-finding protocols and Hierarchical routing protocols. Since flat routing

protocols necessitate maintaining routing table data and cannot aggregate the information, they are not appropriate for large weighing machine sensor networks. Hierarchical routing protocol can solve this problem to some extent.

A wireless sensor network (WSN) consists of a huge numeral of sensing devices, called sensor nodes, which are consistent all the way through wireless links to carry out disseminated sensing tasks. WSNs have establish many functional applications for mechanical data collecting, such as surroundings monitoring, armed forces examination, and objective tracking, for monitoring the behavior of opponent defense force or expensive material goods, in danger of extinction animals. When a sensor node detects a combatant or an endangered living thing, 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 and the wild pandas move in the network, their presence and activities are periodically sensed by the sensor nodes and reported to go under the exterior.

## 2. RELATED WORK

Sensor networks encompass be envisioned to be very practical for a wide assortment of up-and-coming national and services applications [8]. However, sensor networks are moreover confronted with a lot of safekeeping threats such as node finding the middle ground, routing disruption and false data inoculation, since they in general function in unattended, unsympathetic or antagonistic atmosphere [5-7]. For applications like martial observation, adversaries have strong incentives to overhear something on network traffic to obtain valuable asserters. Abuse of such information can source monetary losses or cause danger to human being lives. To look after such information, researchers in sensor network safety measures have been listening carefully, insignificant effort on judgment ways to provide classic security services such as discretion, substantiation, reliability, and availability. Despite the fact that these are critical

requirements, they are insufficient in many applications [4]. The announcement patterns of sensors can, by themselves, reveal a great deal of contextual information, and can disclose the location information of critical components in a sensor network.

### 2.1 Wireless Sensor Networks

A wireless sensor network is a collected works of nodes well thought-out in a network. Each node consists of one or more microcontrollers, CPUs or DSP chips, a recollection and a RF transceiver, a power source such as batteries and accommodates an assortment of sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc approach.

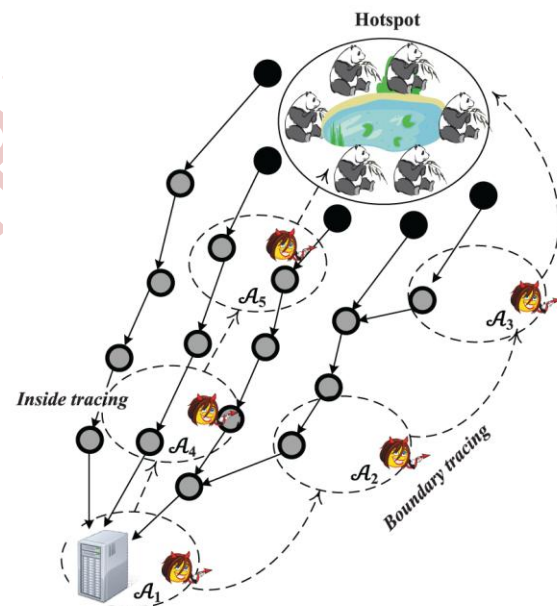


Figure 1: Self organization of boundary tracing

A wireless Sensor Network is a composed works of sensors with imperfect possessions that work in partnership in order to accomplish a widespread aim. Sensor nodes activate in aggressive environments such as encounter fields and observation zones. Due to their operating natural world, [11-14] WSNs are often

unattended, hence prone to more than a few kinds of novel attacks. The mission-critical nature of sensor network applications implies that any conciliation or loss of sensory resource due to a malicious attack launched by the adversary-class can cause significant damage to the entire network. Sensor nodes deployed in a combat zone may have intellectual adversaries operating in their environment, intending to challenge damage or take control messages exchanged in the network [9]. The compromise of a sensor node can lead to greater damage to the network. The resource challenged nature of environments of operation of sensor nodes largely differentiates them from other networks.

## 2.2 Hotspot Incursion

Hotspot attacker who tunnels packets at one point to another point in the network, and then replays them into the network from that point [17][16][15]. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols. Since the tunneled distances are longer than the normal wireless transmission range of a single hop, the source will prefer the path including the attack nodes. Then the attack nodes may perform various attacks, such as the black hole attacks (by dropping all data packets) and grey hole attacks.

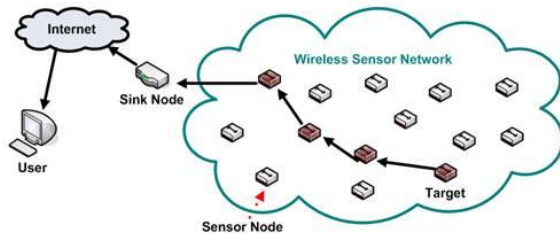


Figure 2: wireless sensor network in access point

## 2.3 Loss Differentiating Automatic Rate Fallback Algorithm

We have explained that when a collision occurs, the data rate should not be reduced. Therefore the modification to the ARF algorithm is that the data rate is

reduced only when a loss of data frame is caused by link errors. Figure 2 describes the new LD-ARF algorithm.

1.If an ACK is received (the transmission is successful) or rate-up timer expires, then,

counter\_downrate = 0;

counter\_uprate ++;

If (counter\_uprate  $\geq$  Nup)

{

physical rate is increased;

counter\_uprate = 0;

rate-up timer is stopped.

}

2. If a NAK is received (a link error loss is detected), then,

counter\_uprate = 0;

counter\_downrate ++;

If (counter\_downrate  $\geq$  Ndown) or the rate was just increased

{

physical rate is reduced;

counter\_downrate = 0;

rate-up timer is started.

}

## 2.4. Network and Adversary models

The sensor nodes are resource-constrained devices with low battery power and computation capacity, but equipped with sensing, data processing,

and communicating components. The Sink has sufficient computation and storage capabilities [10] and its basic function is to collect the data sensed by the sensor nodes. Pandas have embedded RF tags [2] and when a sensor node senses a panda, the node is called source node and generates and sends event packets to the Sink [19]. Each sensor node has a transmission range of  $r_s$  meters and the communication in the network is bidirectional, i.e., any two nodes within the wireless transmission range can communicate with each other [18]. Multi-hop communication is used if the distance between a sensor node and the Sink is more than  $r_s$ , where some sensor nodes (called relaying nodes) act as routers to relay the source node's packets. The Sink is the only destination for all the packets in the network.

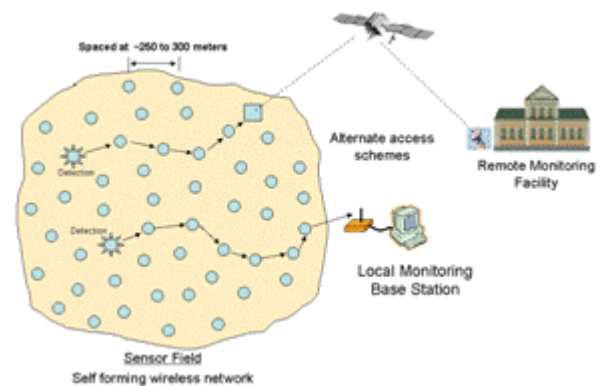
Wireless Sensor Network (WSN) found many applications such as military and security applications, environmental and habitat monitoring, medical application and in data collection. In this paper, we use WSN application for data and habitat monitoring. For example, we are trying to save the particular animal organization say pandas. The movement and the activities of the pandas are regularly monitored and send the information to sink. Since WSN is open source network, the data transmission is not secure. The possibilities of attack are higher which may results in lack of data. In wireless sensor networks, privacy is the most important concern. The privacy threats can be classified into two ways: data-oriented privacy and content privacy. In data-oriented privacy threat, the adversary can observe the packet details and after finding the location of the source the pseudonym packet is inserted. In the content privacy threat, the adversary can eavesdrops on the data transmission in the network and tracks the traffic flow. However the adversary could not interpret the data. Some of the existing methods are based on either routing based model or global model. In the routing based scheme, to avoid the adversary problem the packets are sent from source to sink through different routes. By doing so, the learning of the data by the adversary is made difficult. And also this includes the back-tracing method i.e. the adversary tries to get the information from sink to the source. If the adversary locate the sink, through back tracing the source route can be identified. However, this increases

the need of more paths which results in the increasing of energy and bandwidth.

### 2.5 Random Routing Scheme (RRS)

Traditional routing protocols cannot defend against the traffic analysis attacks because of the nature of regular designed relatively fixed routing. By tracing or tracing back the forwarded packets, adversaries might reach the destination or source. Adversaries also could through observing the packet sending rate derive traffic patterns and allocate base station and source. In order to defend against the traffic tracing attacks, we propose a random routing scheme (RRS), which randomizes the routing path and provides path diversity that means the packets are always forwarded in different directions thus it reduces the traffic pattern analysis ability of the adversaries. And next, we combine RRS with a dummy packet injection scheme which can effectively mislead the adversary into deviating from correct directions. It can be seen that the nodes near of the Sink clearly send a significantly larger volume of packets than the nodes further away, and the packet sending rates gradually decrease as we move to the network edges.

### 3. HOTSPOT PHENOMENON



**Figure 3: Incursion detection**

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 adversary attempts to make use of this traffic inconsistency to locate hotspots to hunt pandas. Thus it illustrates the Hotspot Phenomenon. The average packet sending rate of each sensor node, when there are no hotspots and by using the shortest path routing scheme where 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 are uniformly distributed.

#### 4. CONCLUSION

The adversary moves the monitoring devices to be closer to the hotspot. These procedures continue until the adversary suspects that an area is a hotspot once he observes large drop in the packet sending rates due to passing the hotspot. Another approach for gentrifying a hotspot is by observing that the number of outgoing packets from an area is much more than the number of incoming packets. This attack indicates that even if the adversary does not have global view to the traffic of the network, he can locate hotspots by using traffic-analysis techniques and simple devices. Each relaying node re-encrypts the packet with the shared key with the Sink and replaces the pseudonym with the one shared with the next node in the route. The purpose of adding an encryption layer at each relaying node is to make the packet look different as it propagates from the fake source node to the Sink to prevent packet correlation and by tracing packets to the fake source node which is infeasible. As we have discussed earlier, using cryptosystems it is necessary to prevent packet correlation, and using fake packets can boost source nodes' location privacy preservation. To reduce the overhead, our scheme uses energy-efficient cryptosystems, including hash function and symmetric key cryptography, and avoids the extensively energy consuming asymmetric-key cryptography.

#### 5. REFERENCES

- [1] I. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 8, pp. 102-116, 2002.
- [2] I. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, "Wireless sensor networks: a survey, computer networks", Computer Networks, vol. 38, pp. 393-422, 2002.
- [3] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, and et al., "A line in the sand: A wireless sensor network for target detection, classification, and tracking", Computer Networks, vol. 46, pp. 605-634, 2004.
- [4] "WWWF-the conservation organization", <http://www.panda.org/>.
- [5] Star News, Panda poaching gang arrested, Shanghai Star Telegram, April 2003.
- [6] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing", Proc. of IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp. 599-608, Columbus, Ohio, USA, 6-10 June 2005.
- [7] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "Spins: security protocols for sensor networks", Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.
- [8] M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards statistically strong source anonymity for sensor networks", Proc. of IEEE INFOCOM'08, pp. 51-59, Phoenix, Az, USA, April 2008.
- [9] H. Liu, B. Zhang, H. Mouftah, X. Shen, and J. Ma, "Opportunistic routing for wireless ad hoc and sensor networks: Present and future directions," Communications Magazine, IEEE, vol. 47, no. 12, pp. 103-109, dec. 2009.
- [10] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," SIGCOMM Comput. Commun. Rev., vol. 34, no. 1, pp. 69-74, 2004.

- [11] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wirel. Netw.*, vol. 11, no. 4, pp. 419–434, 2005.
- [12] Z. Zhong, J. Wang, S. Nelakuditi, and G.-H. Lu, "On selection of candidates for opportunistic anypath forwarding," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 10, no. 4, pp. 1–2, 2006.
- [13]. M. Mahmoud and X. Shen, "Lightweight privacy-preserving routing and incentive protocol for hybrid ad hoc wireless networks", *Proc. of IEEE INFOCOM, International Workshop on Security in Computers, Networking and Communications (SCNC)*, Shanghai, China, April 10-15, 2011.
- [14]. Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Networks" *IEEE Trans. Wireless Comm.*, vol. 7, no. 10, pp. 3769-3779, Oct. 2008.
- [15]. Y. Li and J. Ren, "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks" *Proc. IEEE INFOCOM '10*, Mar. 2010.
- [16]. Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks", *IEEE transactions on parallel and distributed systems*, vol. 23, no. 10, pp. 1805-1818, Oct. 2012.
- [17]. R. Lu, X. Lin, H. Zhu, and X. Shen, "Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Comm.*, May 2010.
- [18]. Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient Privacy- Preserving Scheme against Traffic Analysis Attacks in Network Coding," *Proc. IEEE INFOCOM '09*, Apr. 2009.
- [19]. H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," *Computer Networks*, vol. 53, no. 9, pp. 1512-1529, 2009.