Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Survey Paper of Various Attack in Wireless Sensor Network

**Anupam Choudhary** Professor
**Sapna Choudhary** Professor
**Nidhi Patel** Scholar (M.Tech)

***Abstract- With a widespread growth of the applications of WSN, the security mechanisms are also be a rising big issue. One of the most notable challenges threatening the successful deployment of sensor systems is privacy. Although many privacy-related issues can be addressed by security mechanisms, one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy. One important class of sensor-driven applications is to monitor a valuable asset. For example, sensors will be deployed in natural habitats to monitor endangered animals, or may be used in tactical military applications. In these asset monitoring applications, it is important to provide confidentiality to the source sensor's location. In this synopsis, we use a generic asset monitoring application, which we have called the Panda-Hunter Game, as well as refer to a formal model for asset monitoring applications that can benefit from source-location privacy protection. We will also define a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to the large volume of packets originating from a small area. We will also introduce a novel attack called Hotspot-Locating where the adversary uses traffic analysis techniques to locate hotspots with low false positive probability.***

***Index Terms—Wireless sensor network privacy, source-location privacy-preserving schemes, context privacy, and anonymity.***

## I. INTRODUCTION

Due to advances in wireless communications and electronics over the last few years, the development of networks of low-cost, low-power, multifunctional sensors has received increasing attention. These sensors are small in size and able to sense, process data, and communicate with each other, typically over an RF (radio frequency) channel. A sensor network is designed to detect events or phenomena, collect and process data, and transmit sensed information to interested users. Basic features of sensor networks are:

- Self-organizing capabilities.
- Short-range broadcast communication and Multi hop routing.
- Dense deployment and cooperative effort of sensor nodes.
- Frequently changing topology due to fading and node failures.
- Limitations in energy, transmit power, memory, and computing power.

These characteristics, particularly the last three, make sensor networks different from other wireless ad hoc or mesh networks. Wireless Sensor Network (WSN) has opened up new challenges for the researchers.

### 1.1 PURPOSE-

A wireless sensor network (WSN) has been proposed for many useful applications for automatic data collecting [1], [2], [3], such as habitat monitoring, military surveillance, home and business smart environments, better management of cities in areas like traffic control, intelligent transportation, search and rescue, disaster relief, and target tracking, for monitoring the activities of enemy soldiers or valuable assets, e.g., endangered animals. In this research, we will 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 [4]. 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, adversaries can eavesdrop on the open and shared wireless medium and make use of traffic information to locate source nodes to hunt pandas. Therefore, preserving source nodes' location privacy is essential due to the easiness of locating pandas and their furs' large market value, e.g., a piece of a panda's fur was sold in China for $66,500 in 2003 [5].

### 1.2 Overview of WSNs-

Wireless sensor nodes are small, embedded computing devices that interface with sensors/ actuators and communicate using short-range wireless transmitters. Such nodes act autonomously, but cooperatively to form a

logical network, in which data packets are routed hop-by-hop towards management nodes, typically called sinks or base stations. A Wireless

Sensor Network (WSN) comprises of a potentially large set of nodes that may be distributed over a wide geographical area, indoor or outdoor. Wireless Sensor Networks (WSNs) enablenumerous sensing and monitoring services in areas of vital importance such as efficient industry production, safety and security at home as well as in traffic and environmental monitoring . Traffic patterns in WSNs can be derived from the physical processes that they sense. WSNs typically operate under light load and suddenly become active in response to a detected or monitored event.

A Wireless Sensor Network can be generally described as a collection of sensor nodes organized into a cooperatively network that can sense and control the environment enabling interaction between persons or embedded computers and the surrounding environment. Usually a WSN is composed of thousands of multifunctional sensing nodes densely deployed in a large geographical area and one or few base stations or sink nodes connect a sensor network to the users via the Internet or other networks. Each sensor node consists of a CPU (microcontrollers, Micro-processors or DSP) for processing the data, memory for storage, a RF transceiver, usually with a single Omni-directional antenna and a power source like batteries or solar cells. Typical sensors used for such nodes could be temperature, light, pressure, vibration, humidity, sound, radiation, etc. Each of these sensor nodes acquire data, process it and route it to the sink node by multi-hopping as shown in figure1.

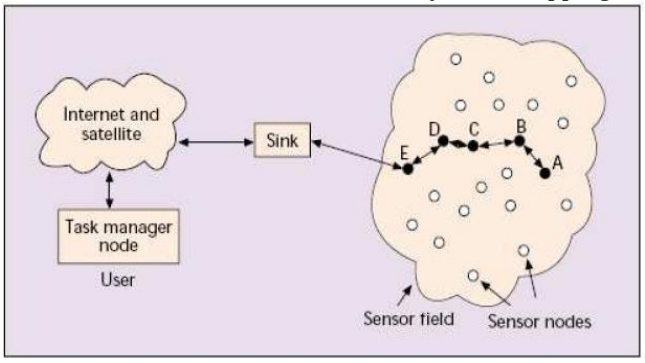



Figure 1: Basic Structure of a Wireless Sensor Network

Though sensor networks provide several advantages and applications, but at the same time pose formidable challenges, such as the fact that energy is a scarce and usually non-renewable resource and the sensor nodes are expected to last until their energy drains out. Since it is not practical to replace the batteries of thousands of sensor nodes, the key challenge will be to maximize the lifetime of sensor nodes. The recent advances in low power VLSI, embedded computing, communication hardware, and in general, the convergence of computing and communications, are making this emerging technology a reality [7]. Likewise, advances in nanotechnology and Micro Electro-Mechanical Systems (MEMS) are pushing toward networks of tiny distributed sensors and actuators.

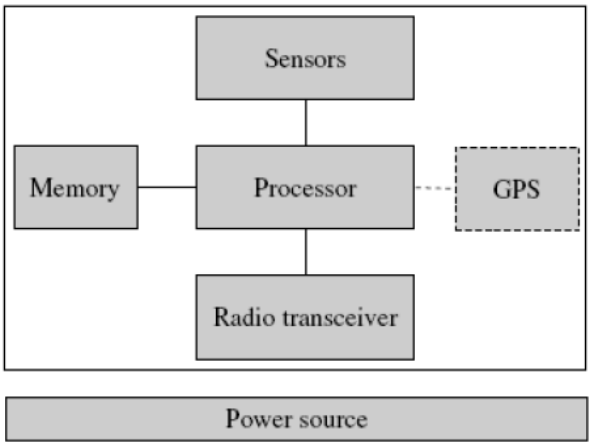



Figure 2: A basic wireless sensor network device block

With the advancement of these low-cost sensors, actuators and wireless technology, WSNs have become attractive alternatives to more traditional wired sensor monitoring in terms of cost, readiness of deployment, robustness and flexibility. There are several key components that make up a typical wireless sensor network (WSN) device as shown in Figure 2.

**1.3 Security Threats and Issues in Wireless Sensor Networks-**

Security is one of the most difficult problems facing by Wireless Sensor Network (WSN).

Although a number of proposals have been reported concerning security in WSNs, provisioning security

remains critical and challenging task. WSNs have attracted much attention due to its great potential to be used in various applications. The list of potential applications that require protection mechanisms includes early target tracking and monitoring on a battlefield; law enforcement applications; automotive telemetric applications; room occupation monitoring in office buildings; measuring temperature and pressure in oil pipelines and forest fire detection. For such applications, security becomes very important. First, wireless communication is difficult to protect since it is realized over a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. Second, since sensor networks may be deployed in a variety of physically insecure environments, adversaries can steal nodes, recover their cryptographic material, and pose as authorized nodes in the network. Third, Sensor networks are vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain a node battery and waste network bandwidth. In these and other vital or security- sensitive deployments, secure transmission of sensitive digital information over the sensor network is essential. The most important security issues in WSN is its inherent security limitations [8] [9].

The privacy threats can usually be classified into :content privacy and contextual privacy[6]. For the content privacy threat, the adversary 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 privacy threat can be countered by encrypting the packets' contents and using pseudonyms instead of the real identities. For the contextual privacy threat, the adversary 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 adversary could not interpret them [7].

The existing source location privacy-preserving schemes can be classified- adversary-based and routing-based schemes. These schemes employ either weak or unrealistic adversary model. The global-adversary-based schemes [8], [9] assume that the adversary can monitor every radio transmission in every communication link in the network. To preserve source nodes' location privacy, each node has to send packets periodically, e.g., at fixed time slots. If a node does not have sensed data at one time slot, it sends dummy packet, so that the adversary cannot know whether the packet is for a real event or dummy data. However, the assumption that the adversary can monitor the transmissions of the entire network is not realistic, especially when the WSN is deployed in a large area. Moreover, if the adversary has a global view to the network traffic, he can locate pandas without making use of the network transmissions. Transmitting dummy packetsperiodically consumes a significant amount of energy andbandwidth, and decreases packet delivery ratio due to increasing packet collision, which makes these schemes impractical for WSNs with limited-energy nodes.

On the contrary,routing-based schemes [6] use weak adversary model assuming that the adversary has limited overhearing capability, e.g., similar to a sensor node's transmission range, and can monitor only one local area at a time. These schemes assume that the adversary starts from the Sinkand tries to locate the origin of a transmission by back tracing the hop-by-hop movement of the packets sent from the source node. Once the adversary overhears a transmission made from node A, he moves to A and waits. Then, he overhears a transmission from node B and moves to B to be closer to the source no de, and so on until he locates the source node.Routing-based schemes try to preserve sourcenodes' location privacy by sending packets through different instead of one route, to make it infeasible for adversaries to trace back packets from theSinkto the source node because they cannot receive a continuous flow of packets. However, if the adversary's overhearing range is larger than the sensor nodes' transmission range, the likelihood of capturing a large ratio of the packets sent from a source node significantly increases. In [6], it is shown that if the adversary's overhearing range is three times the sensor nodes 'transmission range ,the likelihood of locating pandas is as high as 0.97. Moreover, if pandas stay for some time in one location, the adversary may capture enough number of packets to locate the pandas even if the packets are sent through different routes.

In this paper, we first define a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to the large volume of packets originating from a small area. Hotspots can be formed for different reasons, e.g., when pandas have high density or spend some time in one area due to the availability of food, water, shadow ,shelter, etc. Second, we develop a realistic adversary model assuming that the adversary has a partial view to the network traffic by distributing a group of monitoring devices at different observation points. Each monitoring device collects traffic information, including a packet's content, the coordinates of the sending node, and the time of sending the packet. Then, using this model, we introduce a novel attack called Hotspot-Locating, where the adversary tries to make use of the traffic inconsistency caused by hotspots to locate pandas by analyzing the data collected from the observation points using traffic analysis techniques such as the nodes' packet sending rates and packets correlation. Finally, we propose a cloud-based scheme for efficiently protecting source nodes' location privacy against Hotspot Locating attack by creating a cloud with an irregular shape of fake traffic, to counteract the inconsistency of the traffic pattern caused by hotspots, and camouflage the source node within the group of nodes forming the cloud. The fake packets also enable the real source node to send the sensed data anonymously to a fake source node selected from the cloud's nodes to send to the Sink. Cryptographic operations are used to change the packets' appearance at each hop to prevent packet correlation and make the source node indistinguishable because the adversary cannot differentiate between the fake and real traffic, i.e., the cloud's traffic pattern looks random for the adversary. Moreover, tracing the packets back to the source node is nearly impossible because the real traffic is indistinguishable and the real source node sends its packets through different fake source nodes. WSNs may be deployed in areas where human maintaining is impractical and thus recharging or replacing the batteries of sensor nodes may be infeasible. To reduce the energy cost, clouds are active only during data

transmission, the nodes generate fake packets probabilistically, and the intersection of clouds creates a larger merged cloud to reduce the number of fake packets and also boost privacy protection.

Moreover, our scheme uses energy-efficient cryptosystems such as hash function and symmetric-key cryptography and avoids the intensive energy consuming cryptosystems such as asymmetric-key cryptography. It also avoids large-scale packet broadcasting and network-wide packet flooding. In order to determine the tradeoff between the energy cost and the strength of privacy protection, some parameters such as the cloud size can be tuned.

Simulation and analytical results demonstrate that the Hotspot-Locating attack is a severe threat to source nodes' location privacy because adversaries can locate the source nodes using few monitoring devices with low-overhearing range and simple traffic analysis techniques .Routing-based privacy-preserving schemes are vulnerable to Hotspot Locating attack because they leak traffic analysis information, i.e., the adversary can correlate packets and observe the high packet sending rates of the sensor nodes near of hotspots. Our scheme can provide much stronger privacy protection than routing-based schemes because in addition to varying traffic routes, it can conceal the traffic analysis information. Our scheme also requires much less energy than global-adversary-based schemes.

Our main contributions can be summarized as follows:

**1)** we develop a realistic adversary model; **2)** we define a hotspot phenomenon, introduce a Hot spot-Locating attack, and demonstrate that routing-based schemes are vulnerable to this attack; and **3)** we propose a novel scheme for protecting source nodes 'location privacy against Hotspot Locating attack with a low energy cost.

## II. NETWORK AND ADVERSARY MODELS

### 2.1 Network 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. The sensor nodes are interconnected through wireless links to perform distributed data collection. The Sink has sufficient computation and storage capabilities [27] to perform two basic functions: 1) broadcasting beacon packets to bootstrap our scheme; and 2) collecting the data sensed by sensor nodes. Pandas have embedded radio frequency (RF) tags [4], and when a sensor node senses a panda, the node is called a source node and generates and sends event packets to the Sink. Each sensor node has a transmission radius meters and the communication in the network is bidirectional, i.e., any two nodes within the wireless transmission range can communicate with each other. Multi hop communication is employed if the distance between a sensor node and the Sink is more than rS, where some sensor nodes (called relaying nodes) act as routers to relay the source node's packets. The Sink is the sole destination for all the event packets.

### 2.2 Adversary Model

The adversary 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 adversary 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. The adversary analyzes theinformation collected by the monitoring devices to locate pandas or change the observation points, e.g., to be closer to pandas. For example, Fig. 2 shows that the adversary
distributes five monitoring devices in five observation areas namedA1;A2;A3;A4, and A5.

In addition, the adversary has the following characteristics:

**1. Passive.** The adversary launches only passive attacks to hunt pandas and avoids active attacks to be invisible from the network operator. Disrupting the network proper operation is not beneficial for the adversary to make use of the network transmissions to locate pandas. Passive attacks are more dangerous than active attacks in the sense that they are much more invisible and difficult to detect.

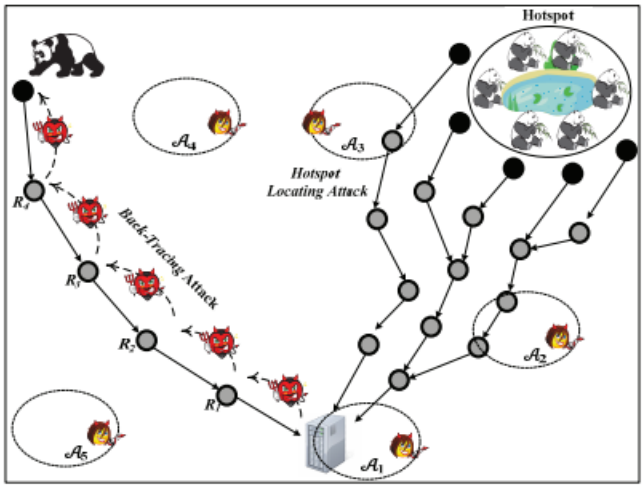
Preserving the location privacy of the Sink is more important in other applications. For example, in military applications, the network is deployed in hostile environment and the adversary aims to locate the Sink to disrupt the network by physically destroying the Sink to prevent the enemy from collecting sensitive information.

2. Well-equipped .Each monitoring device is equipped with supporting equipments such as antenna and spectrum analyzers. It can intercept the packets in the monitored area and measure the angle of arrival as well as the strength of the signal to accurately determine the locations of the nodes that send packets.

However, it cannot determine the location of the receiving node because all the nodes in the transmission range can be the potential receiver of the packet.

The monitoring device's overhearing radius (rA) may be larger than the sensor nodes' transmission radius e.g.,rA¼rSand————————————1, but the adversary cannot monitor the entire network. This is realistic because sensor nodes are cheap and simple devices, but the monitoring devices will be more sophisticated due to the large market value of the pandas' furs. The monitoring devices have sufficient memory for storing all the transmission information in their overhearing range. They also have large energy resource and sufficient computation capability for analyzing the collected data, but it is not sufficient breaking the encryption algorithm or the hash function.3. Informed .The adversary knows the location of the Sink and monitors its traffic because it is the destination of all the event packets. To appropriately study privacy, we apply Kerchoff principle [28] by assuming that the adversary knows the privacy preserving scheme and the used cryptosystems, but does not know the cryptographic keys.




**Cloud-Based Privacy Preserving Scheme**

it consists of 3 phases :

- Pre-deployment Phase
- Bootstrapping Phase
- Event Transmission Phase

**Pre-deployment 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.

It is used to compute a shared key with any sensor node using identity-based cryptography (IBC).

**Bootstrapping Phase**

- This phase is performed only one time in the lifetime of the network.
- It has three main purposes:
- informing the Sink about the nodes locations to link an event to its location.
- assigning fake source nodes and discovering the shortest routes to the Sink.
- Forming groups that are used in creating clouds

**Event Transmission Phase**

- It conceals a source node within a group of nodes with an irregular shape, called "cloud."
- A real source node sends an event packet anonymously to a fake source node to send to the Sink.
- A cloud of fake packets is activated to protect the source node location.
- The nodes of the cloud send fake packets to add randomness to the traffic pattern to :
- make the transmission of the event packet from the real source node to the fake one indistinguishable.
- make the source node indistinguishable by analyzing the packet sending rates of the cloud's nodes.

## III. CONCLUSION

Security is another unique characteristic of WSN and it is a fundamental concern in order to provide protected and authenticated communication between sensor nodes in critical applications, such as military or healthcare. In WSN, physical security of sensor nodes is not granted as they are usually deployed in remote and hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. In order to optimize the conventional security algorithms for WSN, it is necessary to be aware about the constraints of sensor nodes. In this research, the Attacker identifies the hotspot location and it has the location and id information of all nodes within its range through location based DREAM protocol and it attacks the also blocks their communication activity in network. Our protection scheme provides the attack free environment in presence of attacker and it also improves the network performance.

**REFERENCES**

[1] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks", Attacks and Countermeasures", Ad Hoc Networks (elsevier), Page: 299-302, 2003.

[2] C.Y. Chong and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," in IEEE Proceedings, pp. 1247–1254, Aug.2003.

[3] Santi, P. "Topology control in wireless ad hoc and sensor networks" Chichester, England: John Wiley & Sons, 2005.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Ipsita Panda "A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012.

[6] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, " A Cloud-Based Scheme for Protecting SourceLocation Privacy against Hotspot-Locating Attack in Wireless Sensor Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 10, pp. 1805-1818, October 2012.

[7] M. Mahmoud and X. Shen, "Lightweight Privacy Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks," Proc. IEEE INFOCOM '11-Int'l Workshop Security in Computers, Networking, and Comm. (SCNC), pp. 1006-1011, Apr. 2011

[8] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.

[9] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," Proc. Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm), pp. 113-126, Sept. 2005.

[10] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 88-93, 2004

[11] K. Pongaliur and L. Xiao, "Maintaining Source Privacy Under Eavesdropping and Node Compromise Attacks," Proc. IEEE INFOCOM, Apr. 2011.

[12] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm., May 2010.