Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Detection and Prevention of Hotspot Locating Attack using FCN Model for Cloud Computing

**M.S. Rajesh Kumar**
*Research Scholor Department of Computer Science*
*SSM College of Arts and Science*
*Komarapalayam, India*

**Mrs.N.Chandrakala**
*Head & Professor*
*SSM College of Arts and Science*
*Komarapalayam, India.*

***Abstract-A 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. When a sensor node detects an soldieror an endangered animal, and it reports the sensing event to the data collector. And these 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. Therefore, preserving source nodes location privacy is essential. Protecting the location identity means ensuring location privacy. In order to ensure node location privacy the following requirements should be fulfilled: (a) no one knows the exact location of the node, except itself; (b) other nodes, typically intermediate nodes on route, have no information about their distance, i.e. the number of hops, from that node. In Existing System,they can protect the source location through using dummy packets, but only the normal adversary can only confuse to find source location, but the global eavesdropper can easily find out the source location, for this purpose, in this paper we protect the source location privacy (i.e.Hotspot)where the large amount of data can be transmit at that place called as Hotspot.Using cloud-based scheme we can efficiently reduce the bandwidth utilization, node energy cost.***

***Keywords- Wireless sensor network privacy, Probabilistic key sharing, Security.***

## I. Introduction

A wireless sensor network(WSN) consists of a distributed sensors to monitor the physical or environment conditions such as the temperature,pressure,sound,etc..and to pass their data through the network to a main location.Using different sensors,WSNs can be implemented to support many applications including security,industrial monitoring,entertainment,asset management,etc.. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications such as industrial process control monitoring and machine health monitoring,etc,..The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors [1].Each sensor network node has several parts: internal antenna and external antenna, a micro controller, and an electronic circuit. Wireless sensor networks(WSN) consist of a large collection of sensor nodes with each node equipped with sensors,processors and radio transceiver.It have a capable of performing both military and civilian tasks.The cost of sensor node is varying according to the constraints ranging size and cost constraints.The corresponding constraints on resources such as memory,computational speed,energy and communications bandwidth and so on.Many different of attacks exist.We are Protecting and Preventing from these attacks using FCN model.

## II. Hotspot Locating Attack

A hotspot is formed when a large volume of packets are sent from the sensor nodes of a small area,causing an inconsistency in the network traffic.So it may last for some time.The adversary model ucing this traffic inconsistency to locate hotspots to hunt pandas.In this paper,we consider three techniques called as content correlation,time correlation and packet sending rates.However, even if the adversary model scheme uses some simple monitoring devices and it may take some more time to locate a hotspot and could not find the pandas.

## III- Operational Requirements And Security For Hotspot Attack

In existing scheme[2] for preventing hotspot attack is based on global based and routing based.The global adversary based scheme[3] assumes that the adversary can monitor every radio transmission in every communication link in the network.To preserve source node location privacy,each node has to send the packets periodically.If a node does not have sensed data at one time,it sends dummy packets,so the adversary model cannot know whether the packet is real or dummy data.In routing based scheme[4],try to preserve source node location privacy by sending packets through a different route instead of one route to make it infeasible for adversaries.

**ISSUES:**In global adversary based scheme [3], the assumption of adversary can monitor the entire network is not possible, because WSN was deployed in a Large area.Transmitting dummy packets periodically consumes a large amount of energy and bandwidth and decrease the packet delivery time In routing based scheme [4] , adversary overhearing range is larger than the sensor node transmission range.

## IV. Proposed Work

In this paper we propose a cloud-based scheme for protecting source nodes location.It preserve the privacy against hotspot-locating attack by creating a cloud with an irregular shape of fake traffic and a group of nodes forming the cloud.The fake packets[2] also enable the real source node to send the sensed data to a fake source node that have selected from the cloud nodes and it send to the sink.Sink is the network to receive and send the data.The sending and receiving data can be encrypted using cryptographic method.This operations are used to change the packets appearance at each place and it helps to prevent the packet correlation and make the souce node indistinguishable.Because the adversary model cannot differentiate the fake data and real traffic data.Under using one-way key hash function to encrypting the message(ie)is called message digest algorithms (MD5).This algorithm takes as input a message of arbitrary length and produces as output a 128-bit.To reduce the energy cost,the clouds are active only during data transmission and nodes are generate the packets probabilistically.And then the intersection of clouds creates a larged merged cloud to reduce the number of fake packets and it will helps to boost privacy protection.

## V. Performance And Result Analysis

For Assigning Fake Source Node, using fake source node adversary cannot find out the real source location and real data, even global adversary can also not distinguish between the real and fake source node. Introduce fake source which generates false messages to mislead the adversary Fake messages have same length and also encrypted so that an adversary can't differentiate with the actual messages. [4] In existing technique, they use a single path routing, and flooding technology, but these both have require a more energy consumption and required extra hardware and pre-deployment phase. Single path reduces energy, but poor at protecting source location privacy. [5] Flooding is not any better, because the shortest-path is still contained within the flood itself. For using the fake source node, Short-lived fake sources can only draw the hunter away momentarily. [6] A fake source is more effective, but it requires a global overview of network. Source sends its hop count to sink – sink instigates a fake source at a node with the same hop count in the opposite direction. Works best when fake source sends at higher rate than real source, but it requires a large energy budget.

For fake and real source node, if an adversary model could locate a fake source node, he should not found the location of the corresponding real source node.Because each real source node sends its packets through multiple fake sources and each fake source node serves a different real sources.For source node and Sink [7], the Sink has to know the real identity of a source node to know the location of the sensed data, but an adversary model should not know the real identity of a source node. In our scheme, the source node uses dynamic pseudonyms that can be linked to the real identity only by the Sink. Using one identity is not secure because if the adversary model could link the identity/pseudonym to its node only, not to source node's location.

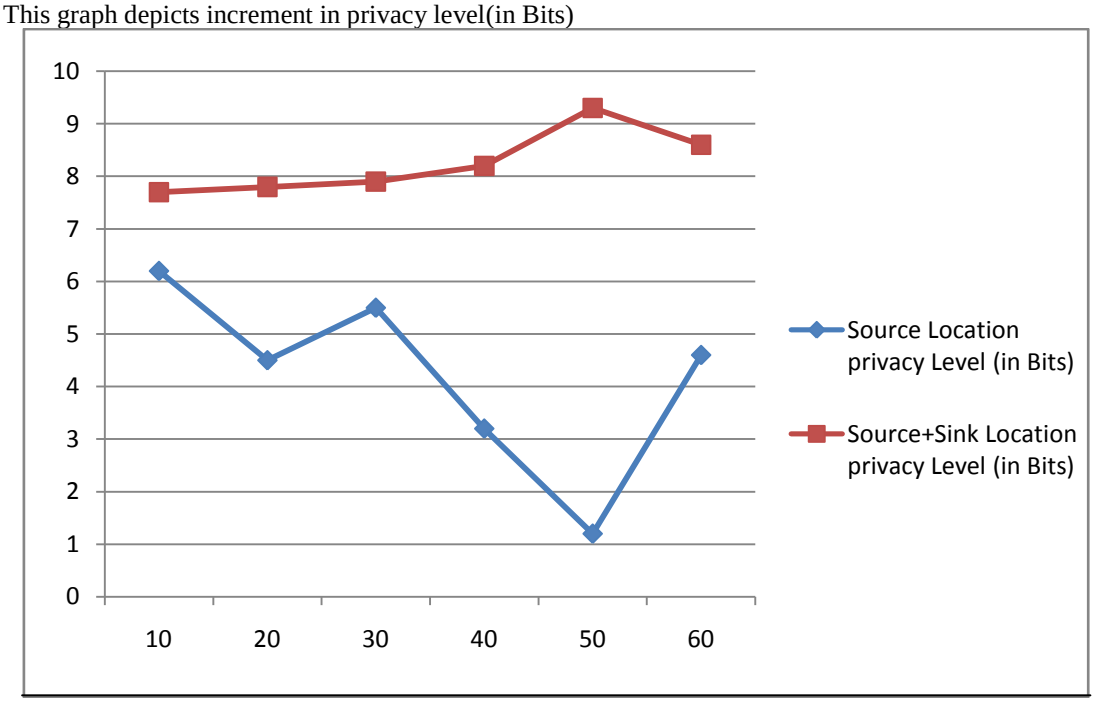
Merging Cloud,using fake source node it require more energy consumption,thereby reducing the energy consumption we use the cloud,if the clouds of source nodes want to sent a packet to node S1 and S2 means these node can be form a cloud like structure thereby after merging the node it can transfer the packet.Cloud merging has two main benefits: 1) lower energy cost: the nodes does not send one fake packet for each cloud and 2) Stronger privacy protection: a merged cloud has a very huge because it has more nodes than the individual clouds. Cloud merging is especially very important for hotspots because it helps to reduce the number of fake packets and boost privacy protection also.

a) Performance Analysis of Existing and Proposed Work

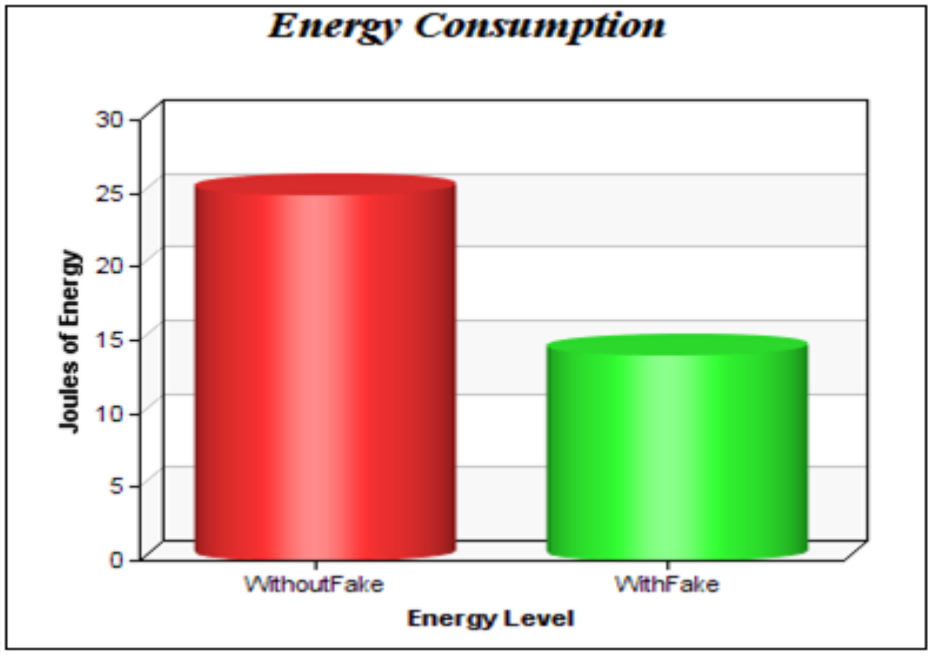
| Nodes | Source ,Sink Location Privacy level(in Bits) | Source,Sink Location Privacy level(in Bits) |
|---|---|---|
| 10 | 6.2 | 7.7 |
| 20 | 4.5 | 7.8 |
| 30 | 5.5 | 7.9 |
| 40 | 3.2 | 8.2 |
| 50 | 1.2 | 9.3 |
| 60 | 4.6 | 8.6 |

b) This graph depicts increment in privacy level(in Bits)




c)This table shows comparision of fake node and without fake node




## VI- Conclusion

Many researchers have worked on FCN model for Wireless Sensor Networks(WSNs) which is a very critical issue from the security point of view.In this paper,Our scheme prevents a source location privacy-preserving that creates a cloud of fake packets around the source node,in varies traffic routes and changes the packets appearance at each hop.We discussed and concluded that even if the adversary model does not have a global view to the network traffic,so we can locate a hotspots using some few monitoring devicesand using simple traffic analysis techniques.Our scheme can provide a strong protection against Hot-spot Locating attack with much less energy cost comparing to global-adversary-based schemes.We can also preserve the both source location and sink data privacy for sink privacy we can use the Sequential Monte Carlo Estimation method to Redistribute and Reshape the Network Traffic. Using this method we can't find out the source location in sink. Every sensor node in the network can collect the information. Sequential Monte Carlo Estimation method can be used to represent the real position of user at each instance.

**References:**

[1] 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.11,pp.3769-3779, Oct..

[2] H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," Computer Networks, vol. 53, no. 9, pp. 1512-1529.

[3] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient Privacy- Preserving Scheme against Traffic Analysis Attacks in Network Coding," Proc. IEEE INFOCOM '10.

[4] W. Trappe and L.C. Washington, Introduction to Cryptography with Coding Theory. Prentice Hall,2002.

[5] 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.

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

[7] X. Cheng, A. Thaeler, G. Xue, and D. Chen, "TPS: A Time-Based Positioning Scheme for Outdoor Wireless Sensor Networks," Proc.IEEE INFOCOM, vol. 4, pp. 2685-2696, Mar. 2004.