International Journal of Advance Research In Science And Engineering http://www.ijarse.com
IJARSE, Vol. No.4, Special Issue (02), March 2015 ISSN-2319-8354(E)

SECURING SOURCE-LOCATION FROM HOTSPOT-LOCATING ATTACK IN WSN

V. Gobinath[1], K. Bergin Shyni[2]

[1]Final Year PG, [2]AP – CSE,

Dr. SivanthiAditanar College of Engineering, Tiruchendur, (India)

ABSTRACT

A wireless Sensor Network (WSN) consists of a huge amount of sensor nodes habitually deployed in spaces where monitoring the substances. Enemies can make use of the traffic information to find the monitoring substances. So, primarily describe a hotspot event that causes an obvious irregularity in the network traffic model due to the huge quantity of packets originating from a tiny area. Second, assuming the adversary can keep an eye on the network traffic in multiple areas rather than the whole network or single area. In this paper, Introduction of novel attack called Hotspot-Locating where the opposition uses traffic investigation techniques to find hotspots. So, propose a cloud-based scheme for resourcefully shielding source nodes location privacy against Hotspot-Locating attack by creating a cloud with an uneven shape of fake traffic to work against the irregularity in the traffic pattern and hide the source node in the nodes forming the cloud. To decrease the energy rate, clouds are active no more than the data transmission time and the meeting point of clouds creates a larger merged cloud to decrease the number of fake packets and also boost privacy preservation. Both the theoretical and simulation study shows that our scheme is more efficient than the global-adversary based schemes and routing-based schemes.

Keywords: Wireless Sensor Networks, Global-Adversary Based Schemes, Routing-Based Schemes, Source Location Privacy

I. INTRODUCTION

A wireless sensor network (WSN) consists of a huge number of sensing devices called sensor nodes which are structured from beginning to end using wireless associations to make circulated sensing tasks. WSNs have many applications for routine data collecting [1] such as atmosphere monitoring, armed observation and target tracking for monitoring the activities of enemy soldiers or precious resources e.g., in risk of extinction animals.

When sensor nodes become aware of a soldier or an endangered animal it reports to the Sink. This data transmit can happen in the course of Multihop broadcast wherever the sensor nodes act as routers.

The privacy threats are naturally classified into: content privacy and contextual privacy [1]. For the content privacy threat the competitor attempts to survey the content of the packets sent in the network to study the sensed data and the identities and locations of the source nodes. This privacy hazard can be countered by encrypting the packets contents and using pseudonyms as a substitute of the real identities.

For the contextual privacy threat the challenger eavesdrops on the network transmissions and uses traffic analysis techniques to deduce sensitive information including whether when and where the data are collected.

The previousmodels for privacy-preserving can be categories into global-adversary based and routing-basedschemes. These methodsoccupy either weak or impracticalchallenger model. The global-adversary-based schemes to protectsource nodeslocation privacy, every node has to send packetsoccasionally.

If a node does not havesensed data at one time slot, it sends dummy packet. But transmission of dummy packets occasionally consumes a considerable quantity of energy and bandwidth, and reduces packet delivery ratio due to rising packet collision.

Routing-based schemes uses weak adversary model assuming that the enemy has restricted overhearing capacity, e.g., similar to a sensor node's transmission range, and can monitor only one local area at a time.

II. RELATED WORKS

2.1Baseline Flooding: In [2] author has proposed the system ofBaseline Flooding is the source node transmitsmessage to each of its neighbours. These neighbours rotatethe message to each of its neighbours and etc. It difficult for an adversary totrace the sourcesince packet is routed from source to destination throughnumber of paths. Adversary can trace the node utilizing backtracking thus this method does not provide much privacy but consumes paramount amount of energy.

2.2 Single Path Routing: In [2] author has explored the Single PathRouting technique in which different from baseline flooding the nodeforwards message only to one of its neighbours.The packetsfrom the neighbours are processed only once.

2.3 Phantom Flooding/ Routing: In [2] the techniques that are proposed by author are the phantom Flooding/ Routing, which achieves locationprivacy by following two phases:

1. Random Walk : message is routed in random fashion for h hops
2. Flooding/Single-path Routing: after h hops message is routed using baseline technique.

2.4 Routing with Fake Messages: The technique that author proposes in [2] is routing done by using fake messages. Fake source will be created by destination when a sender notifies the destination that it has real data to send. These fake senders are far from the real source and more or less at the same distance from the destination as the real sender. Equally real and fake senders start generating packets at the identical time. It has two challenges:

1. How to choose fake source
2. Rate of fake messaging

2.5 Location Privacy Routing Protocol (LPR): The author in [13] discovers on packet backtracking attack and proposes location privacy routing protocol (LPR). In this technique each sensor categories into closer list and a further list by using neighbours. If sensor culls the next hop from closer list then energy efficiency will be more preponderanand and if it culls next hop from the further list, privacy protection will be more vigorous. The retrieval of traffic direction information by the adversary is minimized.

2.6 Source Location Privacy through RRIN: The author proposes the technique RRIN toaccomplish source location privacy in wireless sensor networkby using the theory of dynamic routing in [12]. In this hypothesis each packet is routed through the node which is selected randomly according to the relative location of the sensor node. The intermediate node should be at least some minimum distance far from the source node in order to keep away from the coverage of the source location to the adversary. This system is appropriate for small level sensor network.

III. WIRELESS SENSOR NETWORKS: AN INTRODUCTION

Wireless Sensor networks (WSNs) is a spatially limitless independent sensor to observe the physical or ecological conditions such as heat, noise, stress etc., and to kindly pass their data from side to side the network to a main position which may be a base station or a monitoring station. The WSN is built via a small number of sensor nodes where each node is associated to one or numerous sensors.

3.1 Structure of WSN

Traffic is the communication between any two or more nodes in a wireless sensor network. There are basically three main types of traffics in WSNs as in:

1. Star model: A star network is an interaction of topology where a single base station can send and/or receive a message to a number of remote nodes.
2. Mesh model: the nodes which are present within its radio transmission range are allowed to transfer data in a mesh network.
3. Hybrid model: A hybrid between the star and mesh network provides a strong and flexible relations network while maintaining the ability to keep the wireless sensor nodes power consumption is low.

3.2 Applications of WSN

Wireless sensor networks have gained huge recognition due to their flexibility in solving problems in dissimilar application domains. WSNs have been effectively useful in a variety of application domains such as:

1. Military applications: Wireless sensor networks are possible an essential part of armed command, communications, computing, intelligence, front line surveillance, survey and targeting systems.
2. Area monitoring: When the sensors detect the event being monitored (heat, pressure etc), the event is reported to one of the base stations which then takes suitable action.
3. Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.
4. Environmental sensing: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research.
5. Structural monitoring: Wireless sensors can be utilized to check the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling Engineering practices to monitor assets remotely without the need for costly site visits.
6. Industrial monitoring: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities.
7. Agricultural sector: using a wireless network frees the farmer from the protection of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.

3.3 Characteristics

The characteristics of a WSN include:

1. Power consumption constraints for nodes using batteries
2. flexibility
3. Mobility of nodes
4. Heterogeneity of nodes

5. Scalability to huge scale of deployment
6. Ability to withstand ruthless ecological conditions
7. simplicity of use
8. Cross-layer design

3.4 Types of Attacks on WSN

1. Selective Forwarding: A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node.
2. Sinkhole Attack: Attracting traffic to a specific node in called sinkhole attack. Sinkhole attacks naturally effort through making a compromised node look mainly attractive to surrounding nodes.
3. Sybil Attacks: A single node duplicates itself and presented in the multiple locations. In a Sybil attack a single node presents manyidentities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.
4. Wormholes Attacks: In the wormhole attack an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network.
5. HELLO flood attacks: An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy.
6. Hotspot-Locating Attack: The attacker uses traffic analysis techniques to locate hotspots.
7. Source-Location Attack: Adversaries nodes make use of the traffic details to locate Source node.

IV. NETWORK AND ADVERSARY MODELS

4.1 Network Model

The WSN consists of the Sink and a huge number of standardized panda-detection sensor nodes which are arbitrarily deployed in a region of attention. The Sink has enough calculation and storage space to perform two basic functions:

1) Broadcasting beacon packets to bootstrap our scheme.

2) Collecting the data sensed by sensor nodes.

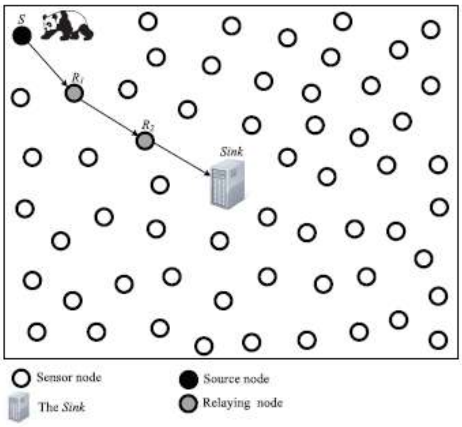

Figure 1 – Architecture of WSN

4.2 Adversary Model

The challenger is a huntsman who eavesdrops on the wireless transmissions and attempts to buildutilize the network traffic to conclude the locations of pandas to track them. The rival organizes a collection of monitoring devices in region of attention called observation points, to gather the traffic information in these regions;however he cannot monitor the traffic of the whole network.

In addition, the challenger has the subsequent characteristics:

1. Passive: The opponent launches only passive attacks to hunt pandas and avoids active attacks to be unseen from the network operator.

2. Well-equipped:Every monitoring device is equipped with supporting equipments such as antenna and spectrum analyzer.

3. Informed: The adversary knows the location of the Sink and monitors its traffic because it is the destination of all the event packets.

V. HOTSPOT-LOCATING ATTACK

A hotspot is created when a huge amount of packets are sent from the sensor nodes of a tiny region causing a clear contradiction in the network interchange which may last for some time.

The fig shows Hotspot-Locating attack.

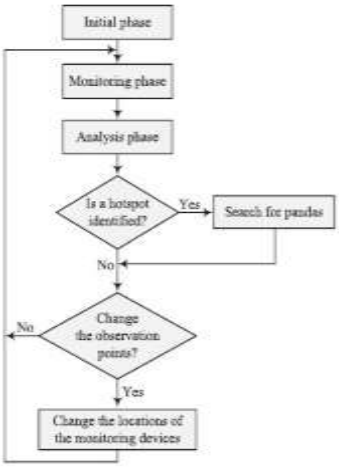

Figure 2 – Hotspot Locating Attack

VI. SOURCE LOCATION PRIVACY

Ourscheme resourcefully protecting, source nodes location privacy against Hotspot Locating attack by designing a cloud with an irregular shape of fake traffic. The fake packets also allow 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 methods are used to modify the packetslook at every hop to avoid packet correlation and construct the source node impossible to differentiatefor the reason that the adversary cannot distinguishamong the fake and real traffic because the cloud’s transfermodel looks unsystematic for the challenger. Furthermore, tracing the packets back to the source node is almostimpracticablesince the real traffic is impossible to differentiate and the real source node sends its packets viadissimilar fake source nodes.

The overall schematic diagram of the source location privacy is shown in fig. the initial step towards the source location privacy is the formation of the network, where the nodes of the network are formed and deployed. The next step to follow up is the designing of an adversary model with the description of the hotspot location, followed by the performance of the hotspot location attack. Then cloud based privacy preservation is performed by the following process.

If a node wants to send a data then the following three steps have to done namely:

1. Pre deployment Phase.
2. Bootstrapping.
3. Merging Clouds.

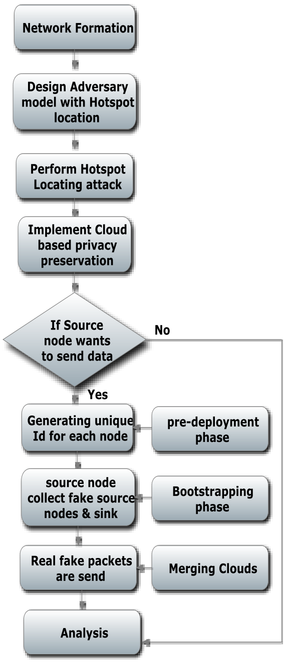
Network Formation
Design Adversary model with Hotspot location
Perform Hotspot Locating attack
Implement Cloud based privacy preservation
If Source node wants to send data
No
Yes
Generating unique Id for each node
pre-deployment phase
source node collect fake source nodes & sink
Bootstrapping phase
Real fake packets are send
Merging Clouds
Analysis

Figure 3 – Overall Schema

In merging the clouds, if a node receives multiple packets from multiple clouds during a short time period, it sends only one fake packet, e.g., for the packet that has superior number of hop counts. If the challenger cannot differentiate the traffic belonging to the individual clouds, the clouds can be merged into a larger cloud for the reason that the challenger will see the nodes of the merged cloud send one packet in a time period.

When a node likes to send a data, it has to generate a unique id for every node. every sensor node X is loaded with a exclusive identity ID_X, a shared key with the Sink K_X, and a secret key d_X that is used to work out a shared key with any sensor node by means of identity-based cryptography (IBC) based on bilinear pairing.

Bootstrapping has three major purposes:

1) Informing the Sink about the nodes locations to connection an event to its location.

2) Conveying fake source nodes and finding the shortest way to the Sink.

3) Forming groups with the aim of used in create clouds.

Cloud merging has two key profits:

1. Lesser energy cost.
2. Stronger privacy protection.

Analysis step is used to analysis overall work and energy cost of the scheme.

VII. THEORETICAL ANALYSIS

The obtainable source location privacy-preserving schemescan be confidential into global-adversary-based and routing-basedschemes. These schemes utilize either weak or idealisticadversary model. The global-adversary-based schemes take for granted with the aim of the enemy know how to keep an eye on each radio transmission in each communication link in the network. To protect source nodes location privacy, every node has to send packets occasionally. If a node does not have sensed data at one time slot, it sends dummy packet accordingly with the intention of the challenger cannot know whether the packet is a realer dummy. Transmitting dummy packets occasionally consumes a considerable quantity of energy and bandwidth, and reduces packet delivery ratio due to rising packet collision, which makes these schemes impractical for WSNs with limited-energy nodes. The routing-based schemes employ weak challenger form assuming that the challenger has restricted overhearing ability, e.g., related to a sensor node’s broadcasting limit, and can supervise only one restricted region at an instance.

Our method preserves a great deal stronger privacy protection than routing-based schemes because in adding together to changeable traffic routes, it can hide the traffic investigation information. Our scheme as well requires much fewer energy than global-adversary-based schemes.

To decrease the energy cost, clouds are energetic minimally the data transmission, the nodes produce fake packets probabilistically, and the junction of clouds creates a superior combined cloud to decrease the amount of fake packets and as well boost privacy protection. Furthermore, our method utilizes energy-efficient cryptosystems such as hash function and symmetric-key cryptography and keep away from the rigorous energy consuming cryptosystems such as asymmetric-key cryptography. It also prevents large-scale packet spreading and network-wide packet flooding. In order to conclude the tradeoff among the energy cost and the power of privacy protection, a few parameters such as the cloud size can be tuned.

VIII. CONCLUSION

In this paper, we first had a conversation on Source Location Privacy, and then we had an introduction to the WSNs and a number of of the applications and a few attacks that can be commonly seen in WSNs. The rest of the paper deals with the Hotspot-Locating Attack in a detailed manner and Source-Location Privacy methods. The theoretical results show that, in most of the scenarios, the Cloud based method is better than the routing-based schemes and the global-adversary-based schemes in terms of energy consumption, computational overhead.

REFERENCES

[1]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, OCTOBER 2012

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing Source Location Privacy in Sensor Network Routing,” Proc. IEEE Int’l Conf. Distributed Computing Systems (ICDCS ’05), pp. 599-608, June 2005.

[3]M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards Statistically Strong Source Anonymity for Sensor Networks,” Proc. IEEE INFOCOM ’08, pp. 51-59, Apr. 2008.

[4]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.

[5]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.

[6]H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," Computer Networks, vol. 53, no. 9, pp. 1512-1529, 2009.

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

[8]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.

[9]K. Mehta, D. Liu, and M. Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," IEEE Trans. Mobile Computing, vol. 11, no. 2, pp. 320-336, Feb. 2011.

[10]B. Alomair, A. Clark,and J. Cuellar, "Statistical Framework for Source Anonymity in Sensor Networks," Proc. IEEE GLOBECOM, Dec. 2010.

[11]Y. Li and J. Ren, "Preserving Source-Location Privacy in Wireless Sensor Networks," Proc. IEEE Comm. Soc.Conf. Sensor Mesh and AdHoc Comm. and Networks (SECON'09), pp. 493-501, June 2009.

[12]Yun Li and JeinRen, "Source Location Privacy Through Dynamic Routing in Wireless sensor Network", Proc. IEEE INFOCOM, 2010.

[13]YingJian, Shigang Chen and Zhan Zhang, "Protecting Receiver Location Privacy in Wireless Sensor Networks", Proc. IEEE INFOCOM, 2007.

AUTHORS

V.Gobinath received her B.E (CSE) in 2013from Mailam Engineering College and pursuing M.E (CSE) in Dr. Sivanthi Aditanar College of Engineering, Tiruchendur. Him area of interest is Network Security in Wireless Sensor Networks and he is also an active student member of CSI.

K.BerginShynireceived the B.E (CSE) and M.E (CSE) in 2009 and 2011, respectively. Her area of interest is Network Security. She is a member of ISTE.