International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 8, Issue 4 (August 2013), PP. 22-25

Assisted Cloud Detection Based Scheme For Discover Hotspot Locating Attack in Wireless Sensor Networks

P.Sasikala, N.Mary, M.P.Subashini
Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Tiruchengode-637205. Tamilnadu, India.
Guided by: Assistant Professor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Tiruchengode-637205. Tamilnadu, India.

Abstract:- Wireless Sensor Networks provides unauthorized person to make use of traffic information located on monitoring of the objects. These sensor networks locate the hotspot incident that causes the inconsistency in the network traffic prototype due to the large volume of packets originating from a small area. We make use of a adversary model assuming that the challenges of the network traffic in multiple areas are monitored, quite than the entire network in one location. In this model, a novel attack call the hotspot location where we use the traffic analysis techniques to locate hotspots. We proposed a cloud based scheme for providing defensive source nodes area privacy, besides from Hotspot-Location attack by developing a cloud with an uneven shapes fake to the traffic, detain the inconsistency in the traffic pattern and locate the source node in which the node forming the cloud. In order to reduce the vigorous cost, the clouds activities during data transmission are maintained and the junction of the clouds with a largest complex cloud are determined to decrease the number of fake packets and also rise privacy safeguarding of the network.

Keywords:- Wireless Sensor Network, Hotspot, Privacy-Preserving Location Monitoring, Back Tracing Attacks, Adversary modal, Network Modal.

I. 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 weighting 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 behaviour of opponent defence 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.

II. 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][6][7]. For applications like martial observation, adversaries have strong incentives to overhear something on network traffic to obtain valuable assert. 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.

A. 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.

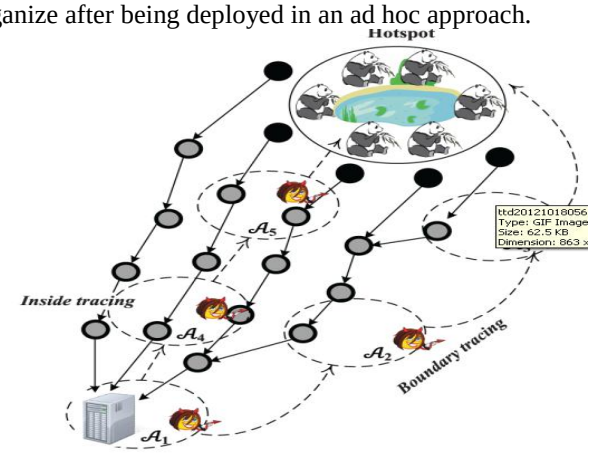

Fig. 1: Self Organization of Boundary Tracing

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][12][13][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.

B. Hotspot Attack

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 tunnelled 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.

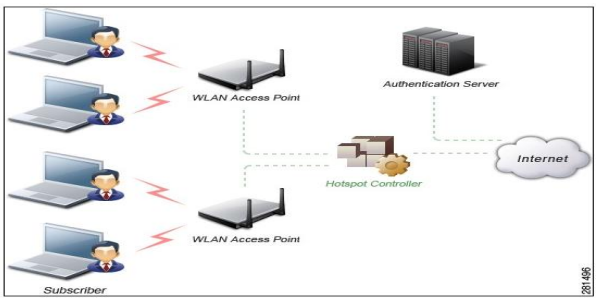

Fig. 2: Wireless Sensor Network in Access Point

C. 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) New LD-ARF algorithm:

- If an ACK is received (the transmission is successful) or rate-up timer expires, then,
  counter_downrate = 0;
  counter_uprate ++;
  If (counter_uprate ≥ Nup)
  {
  physical rate is increased;
  counter_uprate = 0;
  rate-up timer is stopped.
  }
- If a NAK is received (a link error loss is detected), then,
  counter_uprate = 0;

D. 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 rs 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 rs, 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 in 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.

E. 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. In the next subsection, 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.

III. HOTSPOT PHENOMENON

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. That can illustrate the hotspot phenomenon. The average packet sending rate of each sensor node when there are no hotspots and 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.

IV. 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 ingoing 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 make back tracing packets to the fake source node infeasible. As we have discussed earlier, using cryptosystems 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.

REFERENCES

[1] Timothy X Brown Jesse E. James.Jamming and Sensing of Encrypted Wireless Ad Hoc Networks.AmitaSethi University.

[2] Mr.PushphasChaturvediMr.Kunal Gupta.Detection and Prevention of various types of Jamming Attacks in Wireless Networks.Dept.Of Computer Science, Amity University.

[3] Neha Thakur. Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks. Dept. of Software Engineering ,SRM University,Chennai, India.

[4] KwangsungJu and Kwangsue Chung . Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks. Department of Communications Engineering Kwangwoon University, Seoul, Korea ksju@cclab.kw.ac.kr, kchung@kw.ac.kr.

[5] S. Periyanayagi and V. Sumathy.A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks.

[6] Alejandro Proa˜no and LoukasLazos .Packet-Hiding Methods for Preventing Selective Jamming Attacks. Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA E-mail:{aaproano,llazos}@ece.arizona.edu.

[7] T. X. Brown, J. E. James, and A.Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[8] M. Cagalj, S. Capkun, and J.-P. Hubaux.Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[9] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of raitors. In Proceedings of ISIT, 2007.

[10] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper.Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[11] Y.Desmedt.Broadcast anti-jamming systems. Computer Networks.35(2-3):223–236, February 2001.

[12] K. Gaj and P. Chodowiec.FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.