International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Source- Location Privacy Protection Based on Cloud in Wireless Sensor Networks

GAYITHRI N [1], S.LOKESH[2]

[1]*Student, M.Tech-Information Technology, Department of CS&E, The National Institute of Engineering, Mysuru Karnataka, India.*
[2]*Associate Professor, Department of CS&E, The National Institute of Engineering, Mysuru, Karnataka, India*

Abstract - *Wireless Sensor Networks are widely used in many applications. It consists of sensors which collect the different information such as location of the object, privately relevant information etc. Source location privacy is the major problem in wireless sensor networks (WSN). Privacy protection especially source location protection prevents the sensor nodes from revealing valuable information about the target. In this paper, we proposed a scheme based on cloud for protecting source location. In this scheme, multiple sinks are adopted to create many routing path thus changes the packet destination in each transmission. A cloud-shaped fake hotspot is created to add fake packets into the WSN to confuse the adversary and provide a comprehensive privacy location.*

Keywords **- cloud, source location privacy protection, wireless sensor network.**

1. INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensing devices called sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. WSNs are significant in many applications for automatic data collecting such as habitat monitoring, military surveillance, and target tracking, for monitoring the activities of enemy soldiers or valuable assets such as endangered animals. When a sensor node detects a soldier or an endangered animal, it reports the event to the data collector called as *Sink*. This data transmission may occur via multi-hop transmission, where the sensor nodes act as routers. In this paper, we consider habitat 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 While pandas move in the network, their presence and activities are periodically sensed by the sensor nodes and reported to the *Sink*.

Source location privacy is the major problem in wireless sensor networks. WSNs are usually deployed in open and large areas that are unattended and lack of protected physical boundary, which makes the networks vulnerable to security 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. Privacy in sensor networks can be classified into categories: content privacy and contextual privacy. Content privacy refers to the confidentiality of the content of packets transmitted between the nodes in network, which can be threatened by the observation and manipulation of adversaries. This type of privacy can be guaranteed by encryption and authentication. However, contextual privacy associated with communication has not been thoroughly addressed. In contrast to content privacy, the issue of contextual privacy is concerned about the confidentiality of information associated with the measurement and transmission of sensed data, for example, sender/receiver location information, which might be deduced by analyzing network traffic.

Location privacy is one kind of contextual privacy, which is an important security issue and must be protected in many scenarios. Lack of location privacy can expose significant information about the traffic carried on the networks and the physical world entities. This is particularly true when the sensor network monitors valuable assets since protecting the asset's location becomes critical. For example, on a battlefield sensors can detect the movements of soldiers and report them to the headquarters; an attacker may then be able to use intercepted sensor network communications to determine the exact location of opposing soldiers through traffic analysis.

In the paper, we focus on source-location privacy protection. The main contribution of this paper is

1) The proposed scheme randomly selects a sink from multiple sinks in the first phase. The sink selection is useful for changing the traditional traffic mode; altered traffic flow addresses the problem of a back-tracing attack.

2) The scheme adopts the concept of intermediate nodes with a high degree of randomness. The routing paths change dynamically in this scheme, with packets sent to nodes in different candidate regions to alleviate the issue of hotspots to some degree.

3) The network creates fake hotspots and fake branches to complicate the traffic pattern. The scene can also extend the safe time for targets. It improves energy efficiency as much as possible while ensuring the security level. This scheme also demonstrates better performance in source location protection than previous work.

2 PROBLEM STATEMENT

We consider a generic scenario in which a WSN is potentially threatened by a particular adversary, where the adversary seeks to breach the location privacy of a source or sink in the network, where a WSN is deployed for pandas monitoring. The WSN is comprised of a sink node and many sensor nodes among which the packets flow from certain source nodes to the sink. As the WSN is potentially threatened by a particular adversary, where the adversary seeks to breach the location privacy of a source or sink in the network, it is equally important to protect the location privacy of the sources and sink simultaneously. The sensor nodes which monitor the pandas (stationary or nomadic), will act as sources and periodically send reports of their surveillance to a static central controller. Routing strategies are demanded to protect the location privacy of the pandas and the central controller, i.e., the sources and the sink.

3 RELATED WORK

Many techniques have been proposed for the protection of the source location privacy in WSN and have proposed a source location privacy scheme that makes use of the *Panda-Hunter* problem as an application scenario for monitoring-oriented sensor networks where the location privacy is important.

Source-location privacy is provided through broadcasting that mixes valid messages with dummy messages [3] [5]. The main idea is that each node needs to transmit messages consistently. Whenever there are no valid messages, the node has to transmit dummy messages. The rate of the broadcasting is either fixed or probabilistic. In practical situation, the dummy messages could be several magnitudes higher than the valid messages. The goal of broadcasting based schemes is to make it infeasible for the adversaries who are able to monitor the traffic of the entire network to perform traffic analysis and distinguish valid messages from dummy messages. The transmission of dummy messages not only consumes significant amount of the limited energy in the sensor nodes, but also increases the network collisions and decreases the packet delivery ratio. Therefore, these schemes are not quite suitable for large sensor networks.

Routing-based schemes preserve source nodes location privacy by sending packets through different routes to make back tracing the movement of the packets from the *Sink* to the source nodes infeasible. In [7, 8] a random-walk based privacy-preserving scheme, called Phantom, is proposed. Each packet takes a random walk to a random location before it is sent to the *Sink*. However, the scheme fails if the adversary's overhearing range is more than the sensor nodes' transmission range. Moreover, it is very likely that routes will loop around the source node and branch to a random location that is not far from the node. To resolve this problem, the source node can attach the direction of the random walk to the packet header, and each node in the random-walk route forwards the packet to a random neighbour in the same direction. However, once a packet is captured in the random-walk route, the adversary can know the direction information to the source node, which reduces the complexity of tracing the packets back to the source.

Wang et al [13] Present privacy-aware parallel routing scheme to maximize the time of back tracing the packets to the source nodes. A weighted random stride routing that breaks the entire routing into strides is proposed. In[14], dynamically selected nodes in each route modify the packets to make back tracing packets to the source node difficult, but the adversary can trace the modified packets if there are only one or few transmissions.

Fan et al. [15] preserve location privacy by using homo-morphic encryption operations to prevent traffic analysis in network coding. In[16], each cluster header can filter the dummy packets received from the sensor nodes of its cluster to reduce the number of dummy packets. However, the scheme requires much computation overhead due to using asymmetric-key cryptography, and the packet delivery delay is long because the cluster header sends packets with a fixed rate regardless of the number of events it collects.

Mehta et al. [17] formalize the location privacy problem using a global adversary model and compute a lower bound for the overhead required for achieving a given level of privacy protection. The proposed scheme by Alomair et al.[18] can guarantee event indistinguishability by achieving interval indistinguishability, where the adversary cannot distinguish between the first, the middle, or the end of the interval. In [19], dummy packets can be filtered at proxy nodes, and the lifetime of the WSN is analyzed at different proxy assignment methodologies.

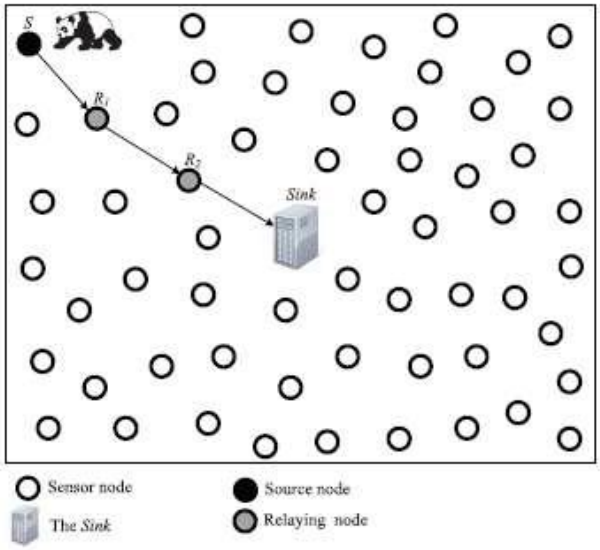

Figure 1 – Architecture of WSN

4 PROPOSED TECHNIQUE

In this paper, we propose a cloud based scheme for preserving source location privacy from source to sink.

It consists of

a. Selecting sink node based on criteria.
b. Selecting Intermediate node.
c. Building a cloud.

First, we choose different destination sink in each transmission to disturb the next movement of adversaries. Altered destination sink can entice the adversaries away from the source location due to difficulty in direction discrimination. The intermediate node is selected to unicast the real packet in a random way. The cloud-like area is created to hide the true location within many fake packets.

5 CONCLUSION

In this paper, a cloud based scheme is proposed to achieve high security performance. This multi-sink strategy makes it difficult for adversaries to trace back packets because the scheme ensures random and safe routing. The destination sink is generally changed per round to hide the source location and packet destination. The cloud centre deployed in the network seeks to complicate detection for the hotspot-seeking adversary. In addition, the cloud shape is irregular; its location and arrangement change each time. The source node sends the real packet per period. The introduction of fake branches defends effectively against the back-tracing adversary. As adversaries are deployed around each sink initially, fake branches in the scheme draw adversaries away from the main path and obscure the traffic flow of the real packet. In addition, the cloud based scheme can protect source privacy under a back-tracing attack and hotspot locating attack.

REFERENCES

[1] Priti C. Shahare, Nekita A. Chavhan "An Approach to Secure Sink node's Location Privacy in Wireless Sensor Networks" Fourth Int'l Conf. on Communication Systems and Network Technologies 2014. pp 748-751.

[2] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in WSNs for the social Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 689–697, 2018, doi: 10.1016/j.future.2017.08.044.

[3] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *DSN '04: Proceedings of the 2004 International Conference on Dependable Systems and Networks*, (Washington, DC, USA), p. 637, IEEE Computer Society, 2004.

[4] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink location privacy enhanced scheme for WSNs through ring based routing," *J. Parallel Distrib. Comput.*, vol. 81/82, pt. C, pp. 47–65, Jul. 2015.

[5] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 51–55, April 2008.

[6] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive Mobile Comput.*, vol. 16, no. A, pp. 36–50, Jan. 2015.

[7] 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.

[8] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing", Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN) in conjunction with ACM Conference on Computer and Communications Security, pp. 88–93, New York, NY, USA, 2004.

[9] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005

[10] J. Wang, F. Wang, Z. Cao, F. Lin, and J. Wu, "Sink location privacy protection under direction attack in wireless sensor networks," *Wireless Netw.*, vol. 23, no. 2, pp. 579–591, Feb. 2017.

[11] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in WSNs

based on path extension," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 461–471, Oct. 2014.

[12] X. Dongliang,W. Xiaojie, L. Dan, and S. Jia, "Multiple mobile sinks data dissemination mechanism for large scale wireless sensor network," *China Commun.*, vol. 11, no. 13, pp. 1–8, Jan. 2014.

[13] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks", Computer Networks, vol. 53, no. 9, pp. 1512–1529, 2009.

[14] K. Pongaliur and L. Xiao, "Maintaining source privacy under eavesdropping and node compromise attacks", Proc. of IEEE INFOCOM, Shanghi, China, April 10-15, 2011.

[15] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy preserving scheme against traffic analysis attacks in network coding", Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

[16] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: Timed efficient source privacy preservation scheme for wireless sensor networks", Proc. Of IEEE ICC'10, Cape Town, South Africa, May 23-27,2010.

[17] K.Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper", IEEE Transactions on Mobile Computing, to appear, 2011.

[18] B. Alomair, A. Clark, and J. Cuellar, "Statistical framework for source anonymity in sensor networks", Proc. of IEEE GLOBECOM, Miami, Florida, USA, 6-10 December, 2010.

[19] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, "Maximizing lifetime of event-unobservable wireless sensor networks", Computer Standards & Interfaces, vol. 33, issue 4, pp.401-410,June2011