Sink Based Privacy In Wireless Sensor Networks Using Clustering

Teslin Jacob
M.Tech Scholar, I&CT Department, Manipal Institute of Technology

Abstract

Privacy in wireless sensor networks is alienated into two main categories they are the data privacy and context privacy. This paper is with reverence to the context privacy. Context privacy includes the contextual information that is location privacy and temporal privacy. Location privacy covers the physical location of the data source and data sink. Our research is with respect to the sink. Suppose the military applications situation. The attacker is quite efficient to monitor the base station and destroy it. So privacy is needed to that of the base station. So a clustered sink mechanism is being presented.

1. Introduction

A wireless sensor network (WSN) is composed of many small sensing devices with limited communication range. The sensors accumulate data from the environment and report them to the base station . With the gifted sensing and wireless technologies, sensor networks are expected to be widely deployed in a broad scale of civil and military applications in the near future [1]. Location information of the sinks, the sensors, and the objects being tracked are very important in sensor networks. Protecting location privacy in sensor networks is critical considering different kinds of attacks that may disrupt the customary function of the networks

To maximize the life period of network, the data should be forwarded such that energy utilization should be balanced among the nodes in fraction to their energy reserved. Privacy in wireless sensor network is divided into data privacy and context privacy. Data privacy is defined as the privacy to the data in the network .Context privacy covers the contextual information which includes the location privacy and the temporal privacy. Location privacy is defines as the information of the location of events in the network .Temporal privacy is defines as the time at which an event is being generated. Location privacy in turn covers the data source and the data sink. This paper is in regard to the data sink. Suppose we take the military applications where in soldiers are being equipped with sensors. They are trying to reach to the base station or the data sink. Now the adversary notices that a large amount of the traffic is being received by the data sink and decides to destroy the base station or the data sink and thereby disabling the complete network. so privacy protection is needed for the base station or the data sink.

The next section presents the related work . Section 3 presents the clustered sink mechanism .Section 5 concludes the paper with areas of open research in the future .

2. Related Work

Recently, location privacy has gained more and more attention. Different approaches are designed to protect users. In location-based services, privacy in location tracking systems [7], [8], [9], [10], is used to determine the user's position. Location broker residing at the middleware layer is used in Spreitzer et al. [7].Hoh et al. [8] create path confusion by crossing paths in areas where at least two users meet. Gruteser et al. [9] disturbs the k-anonymity criterion to meet the sensed location data. Hierarchy of "mist routers" and a handle-based virtual circuit routing protocol is used to preserve the location privacy in Al-Muhtadi et al. [10].eavesdropping and traffic-analysis attacks on the Internet can be protected using anonymous communications in Onion routing [11]. Its goal is to hide the identities of the end hosts in a communication session. onion routing uses different network and threat models that is suitable for location-privacy problem in sensor networks. Furthermore, onion routing is expensive in sensor network because of the large communication/computation overhead.

Passive eavesdropping attacks in mobile ad hoc networks is dealt in MASK [12]. In order to achieve anonymity in communications, it is more concerned about nodes' network/MAC addresses. But packet-tracing attack is not considered here.

The problem of how to hide the location of the base station in a sensor network is dealt in [2], Deng et al. Multi-path routing and fake message injection techniques are introduced here. The base station's location is determined by traffic-analysis attack through the measurement of traffic rates at various locations. It has been pointed out that traffic-analysis attack takes longer time to find a receiver than the packet-tracing attack. Another method has been proposed in [13], Deng et al. Under a certain traffic rate model, to hide the traffic pattern and the parent-child relationship, the transmission times of the packets are randomly delayed. Extra delay for delivering packets is taken in this approach.

To protect the location privacy of source nodes (senders) in a sensor network , [1], [14], a routing protocol called Phantom routing is designed. A random walk is performed by packets before reaching sink. By this makes it is harder for an adversary to trace the movement of packets. There are many source nodes in sensor network, because of this the Phantom routing cannot protect the location privacy of the receiver.

Another approach is a source-sink based random walk is proposed to defend the location privacy of source nodes against a particular type of attacks. This approach cannot protect the receiver, for the same reason that randomized routing alone cannot change the general trend of the traffic as a whole from flowing towards the receiver.

3. Proposed Work

In the majority wireless sensor network (WSN) applications nowadays the entire network must have the ability to operate unattended in callous environments in which pure human access and monitoring cannot be easily scheduled or efficiently managed or it's even not realistic at all [1]. Based on this critical expectation, in many significant WSN applications the sensor nodes are often deployed haphazardly in the area of interest by relatively unrestrained means (i.e., dropped by a helicopter) and they form a network in an ad hoc manner [2,3]. In this section we present the clustered sink mechanism.

Clusters will be formed. There will be a cluster head for each of the cluster. Among the cluster heads in turn there will be cluster head commander who will in turn forward the data to the sinks. Dummy sinks will be simulated in the field that will generate traffic similar to that of the real traffic. Once deployment is done we will place the real sinks and select which are the dummy sinks to be simulated. Once the dummy sinks are selected sensor should then develop the routing paths to send data to places where sinks are simulated.

During network operations whenever a sensor node senses the event then the report is being sent to the dummy sinks. Whenever a dummy sink receives the packet it broadcasts it locally so that the adversary would believe that the real sink could be in that range. There by confusing the attacker.

Privacy

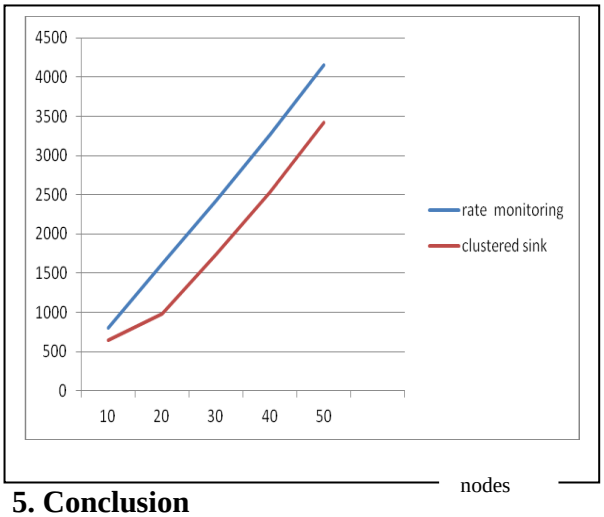
Optimal privacy is achieved with regard to that of the global eavesdropper.

Energy Consumption

Reduced energy consumption is achieved.

4. Simulation Analysis

This is the energy consumption graph for the sink privacy. We see that reduced energy consumption is being consumed. There by confusing the attacker and achieving the privacy.



5. Conclusion

This paper reviews the privacy-preserving techniques for wireless sensor networks (WSN) against a global adversary. Two main categories of privacy preserving techniques have been presented; data oriented and context-oriented respectively. The clustered sink mechanism has proved to give good performance with respect to the energy consumption and message overhead.

6. References

[1] K. Sohraby, D. Minoli and T. Znati. , "Wireless Sensor Network: Technology, Protocols and Applications*:", John Wiley & Sons,* 2007,pg10-11.

[2] C. Ozturk, Y. Zhang, and W. Trappe. "Source-location privacy in energy constrained sensor network routing*": In Proceedings of the 2nd ACM workshop on Security of Adhoc and Sensor Networks*, 2004

[3] R. Agrawal, A. Evfimievski, R. Srikant,, "Information sharing across private databases in:" : *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data*, 2003, pp. 86–97.

[4] L. Sweeney, "K-anonymity: a model for protecting privacy, *International Journal on Uncertainty, Fuzziness and Knowledge based Systems*" 2 (2) (2002) 557–570. pp. 86– 97.

[5] Na Li, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham," Privacy preservation in wireless sensor networks: A state-of-the-art survey". Ad Hoc Networks 7 (2009) 1501–1514.

[6] Jean-Franois Raymond. Traffic analysis: Protocols, attacks, design issues and open problems. *In Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*, pages 10-29. Springer- Verlag New York, Inc., 2001.

[7] Celal Ozturk, Yanyong Zhang, and Wade Trappe, "Source location privacy in energy-constrained sensor network routing". In SASN '04: *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 88-93, New York, NY, USA, 2004. ACM.

[8] Y. Xi, L. Schwiebert, W.S. Shi, Preserving source location privacy in monitoring-based wireless sensor networks, in: *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006)*, April 2006.

[9] Du, W., Deng, J., Han, Y. S. & Varshney, P. (2003),A witness-based approach for data fusion assurance in wireless sensor networks, in '*IEEE Global Communications Conference* (GLOBECOM)', Vol. 3,pp. 1435– 1439.

[10]He, T., Vicaire, P., Yan, T., Luo, L., Gu, L., Zhou, G., Stoleru, R., Cao, Q., Stankovic, J. A. & Abdelzaher, T. F. (2006), Achieving real-time target tracking usingwireless sensor networks., in 'IEEE Real Time Technology and Applications Symposium', *IEEE Computer Society*, pp. 37–48.

[11]Hu, L. & Evans, D. (2003), Secure aggregation for wireless network., in 'SAINT Workshops', *IEEE Computer Society*, pp. 384–394.