Protecting Location Privacy in Wireless Sensor Networks against a Local Eavesdropper – A Survey

Chinnu George
M.Tech Scholar
Karunya University

Dhinakaran Nathaniel
Assistant Professor
Karunya University

ABSTRACT

This paper presents the review of the existing privacy techniques in wireless sensor networks (WSN). There are two main categories of privacy preservation in WSN. They are data privacy and the context privacy. This paper presents the context privacy. In context privacy we focus on location privacy. Location privacy is defined as the location of the events. Location privacy is thus of the utmost importance. Failure to protect the physical location can cause loss of the information and subvert the entire network. Thus protection of the physical location is needed at data source and the data sink. Suppose we take the scenario of the panda – hunter where in sensors are being deployed in the forest to monitor the endangered pandas. The adversary is quite efficient to monitor the panda and capture the panda. So an analysis of the existing techniques against a local eavesdropper is being presented. This paper should be helpful for the research in privacy preservation in WSN in the future work.

General Terms

Wireless Sensor Network.

Keywords

Privacy, Data mining.

1. INTRODUCTION

A wireless sensor network(WSN) is built of the sensor nodes . These nodes vary from few to hundreds to several thousands. Sensors are capably of monitoring the physical location, temperature, vibration, sound ,etc and send to the base station. The sensor nodes are prone to failures this can be due to the battery, overhead etc. A lot of work has been done to increase the performance of the power and resources using different routing algorithms however now there is need of the privacy of the individuals.

There are number of the applications in the WSN. This includes [1]the military applications which controls the monitoring, tracking and surveillance of the borders. Other applications include the environmental applications, health applications, home applications, commercial applications.WSN are capable to collect their data automatically with the help of the sensor devices. Even though there is great benefit to the users some misuse them so privacy is a concern there. If we take famous scenario of the panda and hunter [2], the hunters can physical location of the panda by monitoring the traffic or using sound monitoring where in panda is tracked with help of the sound recognition.

So a design of the new technologies should be taken into account against privacy. In this paper a review of the existing privacy techniques in WSN has been presented. There are two main categories of the privacy preserving techniques ; data privacy and context oriented privacy. The data privacy focuses on privacy of the data so that no modification is done to the data. The context oriented privacy focuses on the contextual information this includes the location information or time of the event. This paper is with respect to the context oriented privacy. In context oriented privacy we focus on the location privacy. At the end some issues are presented which would be helpful for future research in privacy in WSN.

In the next section a introduction to the existing approaches is given. Section 3 presents the privacy preservation techniques with respect to context privacy. In context privacy we focus on the location privacy. The different techniques are compared and also presents open issues for future research in section 4 followed by the concluding remarks in section 5.

2. RELATED WORK

Privacy is a critical issue in field of the networks, data mining, and other fields. Many techniques have been proposed for the privacy preservation in WSN such as: cryptographic security [3], k-anonymity [4]. But these techniques were used to protect the data when it flows from one node to other. A large number of the attacks have been possible in WSN. This includes the Sybil attacks, Traffic analysis attacks, physical attacks, DOS attacks. Our area of interest is on attacks with respect to privacy.

Privacy in WSN can be classified into two categories data oriented and context oriented privacy. Fig. 1 shows the classification of privacy in WSN.

3. PRIVACY PRESERVING TECHNIQUES

This section deals with two most important branches of the privacy preservation techniques data oriented privacy and context oriented privacy. Data oriented privacy focuses on the data that is being collected and then send to the sink. Context oriented privacy is the contextual information like that of the physical location or time of the event.

.

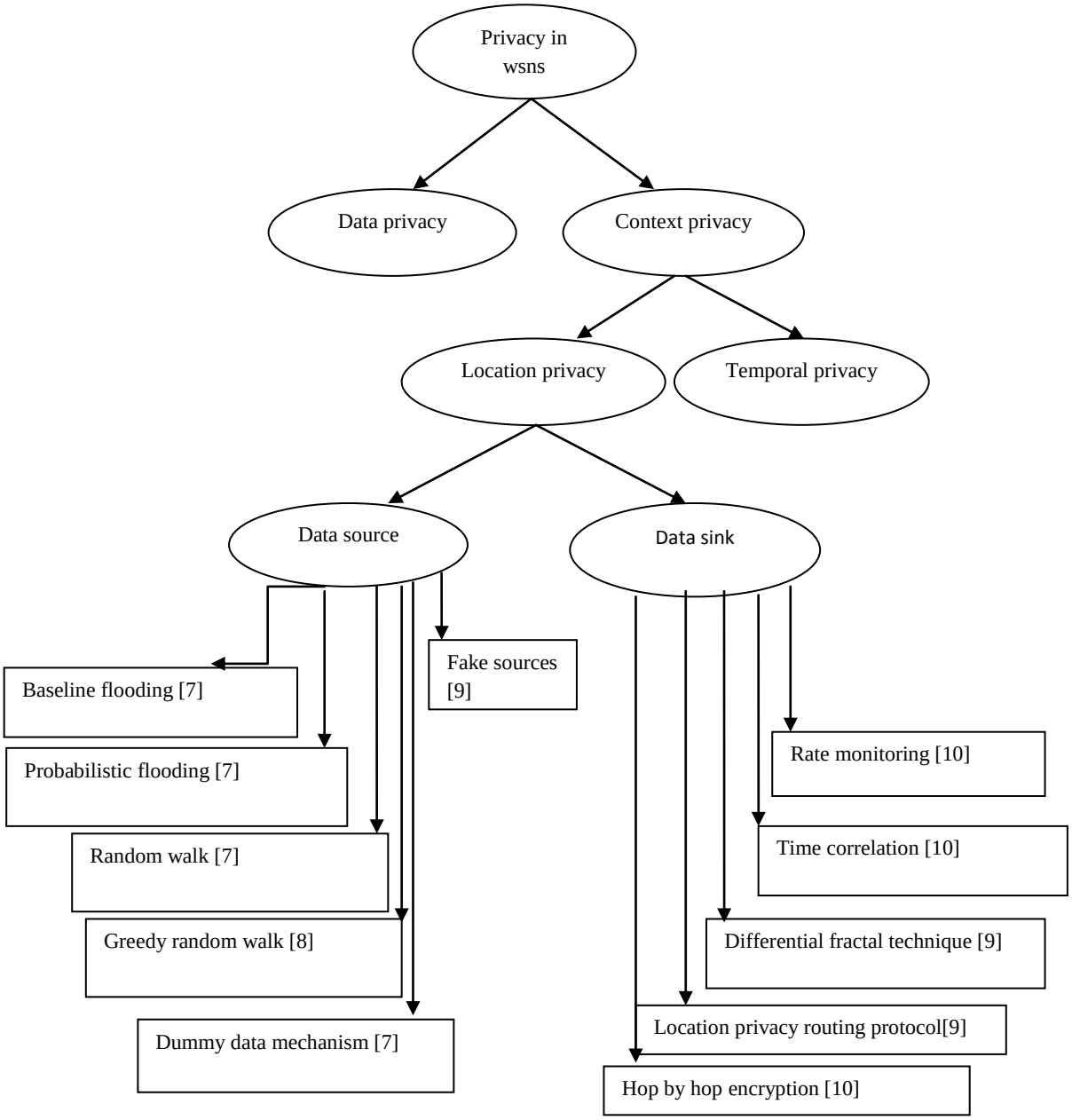

Figure 1 Classification of the privacy preserving problems for WSN.

We mainly focus on the context oriented privacy.

3.1 Context - oriented privacy preservation techniques

Although privacy is achieved with different protection techniques, the sensor nodes are so sensitive that it needs to be protected. The adversary can use traffic analysis techniques [6]. Context oriented privacy is summarized in the next two sections.

3.2 location privacy

Location privacy is a critical issue in WSN especially in the case of the hostile environments. Failure to such physical location can subvert and disable the network there by allowing the adversary to launch attacks. The famous panda hunter problem [2] where in the sensor are deployed in the forest. Sensor nodes are used to find the physical location of the panda in their local habitat. Adversary can find the location of the sensor node that monitor the panda and thereby capture the panda. Location privacy is further classified into two main categories; location privacy of data source and location privacy of data sink.

3.2.1 Location privacy for the data source

Suppose we take a scenario of the famous panda – hunter problem where in sensors are being deployed in the forest. The hunters are monitoring and thereby capturing the panda. A sensor node detects the presence of the panda and sends to the base station with the help of the multihop communication while rest of the sensor nodes being idle. The hunter now sees that the base station has received the presence of the panda and would like to know the exact source. The hunter can use the backtracking procedure or the traffic analysis and find the exact location of the data source. So privacy protection is needed at the data source.

Flooding [7] has been used to preserve the physical location of the data source .In the case of the baseline flooding mechanism. a sensor node detects the presence of the panda and broadcasts it to its neighbors. These neighbors in turn broadcast to their neighbor and finally being received by the base station. The hunter notices that the base station receives multiple copies of the same message. And thereby confusing the hunter or the adversary. However the effectiveness of the base lining flooding depends on the no of nodes on the transmission path between the data source and base station. If the path is too short then the hunter can use the shortest path between the data source and base station.

To address the consequence of the baseline flooding, probabilistic flooding is proposed in [7], in this mechanism not all sensors are involved in the forwarding data rather each node broadcasts with a Preset probability .This scheme reduces the energy consumption but there is no guarantee of the reception data by the base station due to the randomness involved this mechanism.

Higher level of privacy can be achieved with the help of the random walk mechanism [7] where in phantom routing is used . In this a random walk is performed from the data source , and then a probabilistic flooding scheme is then used.fig2 . shows the random walk mechanism.

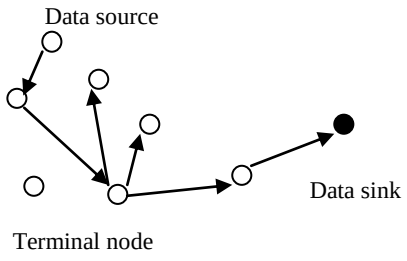

Figure 2 Random walk mechanism

Another higher level technique is the greedy random walk [8] where in the base station first initializes a random path with a given number of the hops. Sensors on this particular path are called the receptors. Then a packet is randomly forwarded from the data source until they reach one of the receptors. Thereby then following the pre established path by the base station. Fig3. shows the greedy walk mechanism.

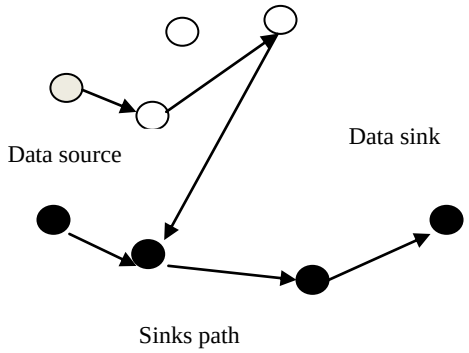

Figure 3 Greedy walk mechanism

To further protect the physical location of the data source dummy data mechanism is used .In this fake packets are introduced to disturb the traffic .a simple scheme of the short lived fake source routing is proposed [7] where in each sensor sends a fake packet with a pre determined probability. Upon receiving a fake packet , a sensor node just discards the packet and upon receiving the real packet it forward to the base station. However energy efficiency is maintained but the length of the each path for the fake path is one hop. Therefore the hunter or the adversary can discard the fake paths and reach to the physical location of the data source .

A still higher level of privacy is achieved with the help of the fake sources mechanism [9]. In this mechanism one or more sensor nodes are chosen to simulate the behavior of the real data source in order to confuse the adversary .however the power consumption is quite high.

3.2.2 Location privacy for base station

Since base station collects the entire data from the network so location privacy is needed at the data sink. Suppose the scenario of the military application where in the soldiers are equipped with the sensors. The soldiers detects the presence of the enemy and send it to the base station using mutihop communication , now the adversary notices that the base station receives large amount of the traffic and there by decides to destroys the base station and thus disabling the whole network . Hence the protection of the base station is very important.

There are different traffic analysis techniques [10] .This includes the time correlation attack where in the adversary observes the correlation in the sending time between a node and the neighbor node who is assumed to be forwarding data and then deduces the path to the base station. Another technique is rate monitoring attack where in the adversary monitors the packet sending rate of the nodes and then moves closer to the nodes that have highest packet sending rate.

Another privacy technique is the differential fractal propagation technique, where in a sensor node sends a real packet , its neighbor node generates the fake packet. The fake packet then travels a given number of the hops . They also design a scheme for creating some areas of the high activity called the hotspots. If such an area receives a packet it creates a high area of the activity and there by local eavesdropper being deceived to this area . But the packet may not be necessarily in this area. And thereby the adversary being confused.

Another approach is the location privacy routing protocol that provides privacy protection to the destination with a given number of the hops also fake packets are generated to the destination .the packets may move close either closer or away from the destination .the fake packets are generated so as to confuse the adversary .

Yet higher level of privacy is achieved with the help of the hop by hop encryption technique where in data encryption technique the packet is re-encrypted hop by hop when its transmitted to the base station. Thereby by not disclosing the base station location through changing the appearance of the data .Yet higher level of privacy is achieved with the help of the hop by hop encryption technique where in data encryption technique the packet is re-encrypted hop by hop when its transmitted to the base station. Thereby by not disclosing the base station location through changing the appearance of the data .

4. COMPARISONS

In this we compare all the privacy preserving techniques that have been reviewed in this paper. Table 1 depicts the performance of privacy preservation techniques in WSNs.

We evaluate their performances in metrics: privacy, accuracy, delay time, and power consumption, location, adversary, message overhead, scalability. Privacy refers to the degree of privacy protection provided by the reviewed techniques. The accuracy measure covers two perspectives: (i) the accuracy of the data obtained by the base station; and (ii) the availability of the (intended) data to the base station (i.e., whether the data can be delivered to the base station). The delay time includes both the computation and communication time of data transmission at the intermediate sensors. The power consumption measure focuses on the additional messages required for transmission (i.e., additional energy consumed) in the WSN.

There are some open issues for future research. As the network behavior changes so sensor nodes should be designed accordingly, along with it there can be improvement in every technique with respect to overhead, power , accuracy.

Table1:Comparison between different techniques

Techniques	**Location**	**Privacy Preservation and Efficiency**	**Adversary**	**Message Overhead**	**Power Consumption**	**Accuracy**	**Delay**
Baseline flooding	source	excellent	Local	No extra over head	High due to flooding of data in network	Guaranteed data arrival	No extra head
Probabilistic flooding	source	good	Local	Small	Low as compare to flooding	No Guaranteed data arrival	Delay can increase
Phantom flooding	source	excellent	Local	Small	Low as compare to flooding	No Guaranteed data arrival	Delay can increase
Greedy walk	source	excellent	local	medium	No extra power consumed	No Guaranteed data arrival	No extra delay
Fake sources	source	excellent	Local	Huge	No extra power consumed	No influence on data arrival and accuracy	No extra delay
Dummy mechanism	source	excellent	Local	Huge	No extra power consumed	No influence on data arrival and accuracy	No extra delay
Rate monitoring	sink	fair	Local	Huge	No extra power consumption	No influence on data arrival and accuracy	No extra delay
Time correlation	sink	fair	Local	Fair	No extra power consumption	No influence on data arrival and accuracy	No extra delay
Differential fractal propagation	sink	fair	Local	Fair	No extra power consumption	Guaranteed Data at sink	No extra head
Location privacy routing protocol	sink	good	Local	Fair	No extra power consumption	No influence on data arrival and accuracy	No extra head
Hop by encryption	sink	excellent	Local	Fair	No extra power consumption	No influence on data arrival and accuracy	Delay due to encrypting and decrypting data

5. CONCLUSION

This paper presents a review of privacy-preserving techniques for wireless sensor networks (WSN) against a local eavesdropper. Two main categories of privacy preserving techniques have been presented; data oriented and context-oriented respectively. The existing techniques have been compared in terms of context privacy preservation with respect to efficiency, overhead, delay, power consumption adversary, location, scalability against a local eavesdropper. In future these techniques can be modified and can be used to protect against a global eavesdropper who has a global view of the traffic at a time.

6. ACKNOWLEDGEMENT

Our thanks to the experts who have contributed towards the development of this paper.

7. 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] K. Mehta, Donggang Liu, and M. Wright. "Location privacy in sensor networks against a global eavesdropper". In IEEE International Conference on Network Protocols, 2007. ICNP 2007, pages 31-323, October 2007

[10] Jing Deng, Richard Han, and Shivakant 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, pages 637-646, Washington, DC, USA, 2004.IEEE Computer Society.

[11] Yi Ouyang Zhengyi Le, Guanling Chen, James Ford, and Fillia Makedon.,"Entrapping adversaries for source protection in sensor networks". In WOWMOM '06: Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, pages 23-34,Washington, DC, USA, 2006. IEEE Computer Society.

[12] Jing Deng, Richard Han, and Shivakant 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, pages 637-646, Washington, DC, USA, 2004. IEEE Computer Society.

[13] Y. Jian, S. Chen, Z. Zhang, and L. Zhang,"Protecting receiver-location privacy in wireless sensor networks." May 2007, pp. 1955-1963.

[14] D. Liu and P. Ning, "Establishing pair wise keys in distributed sensor networks," in Proceedings of 10th ACM Conference on Computer and Communications Security (CCS03), October 2003, pp. 52–61.