Privacy Preserving Techniques In Sensor Networks To Protect Location Information

Dr.B.Raveendranadh Singh, Professor of CSE & Principal of Visvesvaraya College of Engineering & Technology,
M.P.Patelguda(V), Ibrahimpatnam(M), R.R.Dist, Hyd-501510.

Sensor networks are widely used for varies real world applications like monitoring wildlife habitat, discovering happening in unmanned areas and so on. Such networks are resource constrained and prone to security vulnerabilities. Adversarieslaunch attacks to exploit the sensitive information being flown in the network. The existing solutions provide confidentiality for the messages being flown in the network. However they could not protect contextual information which can be exploited by adversaries and derive useful information like the location of sensors, data sinks and monitored objects from that. Existing solutions avoid leakage of location information from an adversary who operates from a small region. These techniques cannot withstand against a global eavesdropper. Recently Mehta, Liu and Wright proposed a strong adversary model for sensor networks that can be used to achieve location privacy. They have provided techniques for source-location privacy and sink-location privacy. In this paper we implement those techniques to study trade-offs between latency, communication cost and privacy. We built a prototype application that demonstrates the proof of concept. The empirical results revealed that the techniques are effective.

Key Words – Sensor Networks, Location Privacy, Global Eavesdropper

INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used to monitor physical world in many real time applications. A WSN is made up of a set of small, wireless devices that perform many functions but resource constrained. The devices are self-organized and they participate in monitoring surroundings [1]. When the monitoring is infeasible or impossible by humans, such real applications use sensor networks. The applications include target tracking, monitoring wildlife habitats, military surveillance and so on. In case of sensitive WSN applications adversaries have strong interest in eavesdropping. They wanted to abuse sensitive information for personal gains. To overcome this problem many researchers provided solutions to protect such networks with security services for availability, integrity, authentication, and confidentiality. These security considerations are proved insufficient in many real world applications. The reason behind this is that they are unable to protect contextual information from which hackers derive sensitive information. The location information of monitored objects and sinks are exploited by adversaries. In this paper these two location privacy problems are explored. We assume that the sensor nodes are not compromised. One of the real world applications of WSN proposed in [2] focuses on Panda-Hunter scenario that tracks endangered giant pandas in a forest where bamboos are grown. It is assumed that each Panda has a tag electronically associated with it which will be able to send signals to sensor network. The sensor nodes that detect these signals forward them to sinks. As the Pandas are monitored objects adversaries can gain the location of the Pandas and cause harm to them illegally. When location of sinks is disclosed, the adversaries can make physical attacks on them to destroy the WSN. In this context, it is very important to protect location privacyof monitored objects and also the sinks. Many methods came into existence to solve the problem. All methods have kept the energy constrained nature of WSN. They also tried to be energy efficient as the energy in WSN is very expensive [3]. These schemes can be defeated by global eavesdroppers who are highly motivated. They may also employ their own sensor nodes to extract sensitive information being flown in the network [4]. In case of military and other such sensitive applications, this is really true.

In this paper, we focused on the techniques that can protect location privacy of both monitored objects and also sinks. The location of monitored objects may be very useful to adversaries to make benefits out of it. In the same fashion the location details of sinks also help adversaries to launch physical attacks on them to destroy the whole network. This is because the global eavesdroppers are highly motivated as they gain monetary and other benefits out of it. For this reason this paper focuses on the adversary model that is based on global eavesdroppers who have a total view of network. The remainder of this paper is structured as follows. Section II provides review of important literature. Section III focuses on the proposed adversary model and solution. Section IV presents experimental results while section V concludes the paper.

RELATED WORKS

With respect to wireless sensor networks, the location privacy plays an important role. Not only securing the data communications, but contextual information also important for the protection. Thus the location privacy is an active area of research for many years. There were many techniques used earlier includingprivate information retrieval [5] andK-anonymity [6]. From user devices by observing wireless signals, the location information is compromised [7], [8]. Other solutions to reduce the problem include dummy traffic introduction and random delay. The location privacy of sensor networks also comes under the general location privacy problems. However, sensor networks throw some unique challenges which are not with other networks. First, the nodes in sensor networks are resource constrained and their lifetime is limited. Second, sensor networks are usually larger with more number of nodes to cover the area under study. Source location privacy has thus assumed significance in the context of wireless sensor networks. Prior works in these areas focused on increasing the safety period before the objects' location is found by attackers [2]. Flood [9] technique is used in WSN to send packets through different nodes to avoid location privacy disclosure. In [2] fake packet generation technique is also used to deceive adversaries. In the same paper phantom single-path routing also achieved location privacy by using random paths before finally reaching sink. In [10] Cyclic Entrapment was explored where loops are introduced to deceive adversaries and thus increase the safety period to send information to sink.

All the techniques mentioned above use a local eavesdropper model. However, in the real world adversaries with higher reach of network may cause threat. For this reason global eaves dropper models assumed importance. Of late many techniques came into existence to model global eavesdroppers in to the security mechanisms of WSNs.Proxies are used by Yang et al. to avoid global eavesdropping [11]. Under a global eavesdropping model, Shao et al. proposed a technique that reduces location privacy problems [12]. From protecting sinks from local eavesdroppers Deng et al. [13] presented a technique that makes use of hashing in the packet header. In [14] it is understood that adversaries can use rate monitoring and time correlation attacks to find out the location of tracks. As explored in [14] these attacks can be prevented using techniques like hot spots, random fake path, and controlled random walk. Fake packets and redundant hops were introduced in [15] that assume local eavesdroppers. However, these schemes can be defeated by global eavesdroppers and find the location information of sinks and monitored objects. In this paper we focus on techniques pertaining to privacy preserving to prevent attacks from global eavesdroppers.

PROPOSED NETWORK AND ADVERSARY MODEL

In this paper we assume a wireless network that has number of sensor nodes that have multiple functionalities and sinks that collect data from mobile sensor nodes. The nodes might be in clusters to be more energy efficient. This is because the nodes in WSN are energy constrained and their life time is limited. The network looks like the one presented in figure 1.

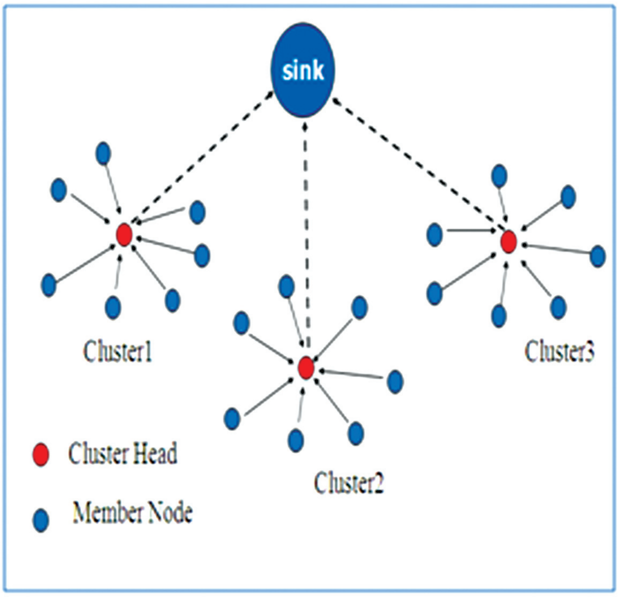


Fig. 1 – Samp le sensor network

As can be seen in the sensor network presented in figure 1, the nodes are sending data to sink. The data is protected generally but the contextual information can be derived from adversaries to get sensitive information. Two kinds of problems are identified here. The first problem is that the adversaries can get location information of the monitored objects. The second problem is that the adversaries can get location information of sinks. In the first case, the adversaries can have strong motivations while the second case gives them opportunity to destroy the sinks physically and thus destroy the whole network and its purpose. We also assume that the nodes are not compromised by adversaries in this paper. The attacker model we proposed keeps global eavesdroppers in mind. It focuses on source location privacy and sink location privacy. The location privacy of the proposed system is defined as follows.

$$b=\sum_{|S_T|}-\frac{1}{|S_T|}\log_2\frac{|S_P|}{|S_T|}=\log_2\frac{|S_T|}{|S_P|}.$$

The optimal location privacy is computed as follows.

$$b\leq\log_2\frac{|S_T^*|}{|S_P|}=\log_2\frac{N}{|S_P|}.$$

The communication cost of source location privacy is estimated as follows.

$$\omega_T=\sum_{i=1}^{\frac{T}{\alpha\times\Delta}}M_s(i),$$

In the same fashion, the sink location privacy is estimated as follows.

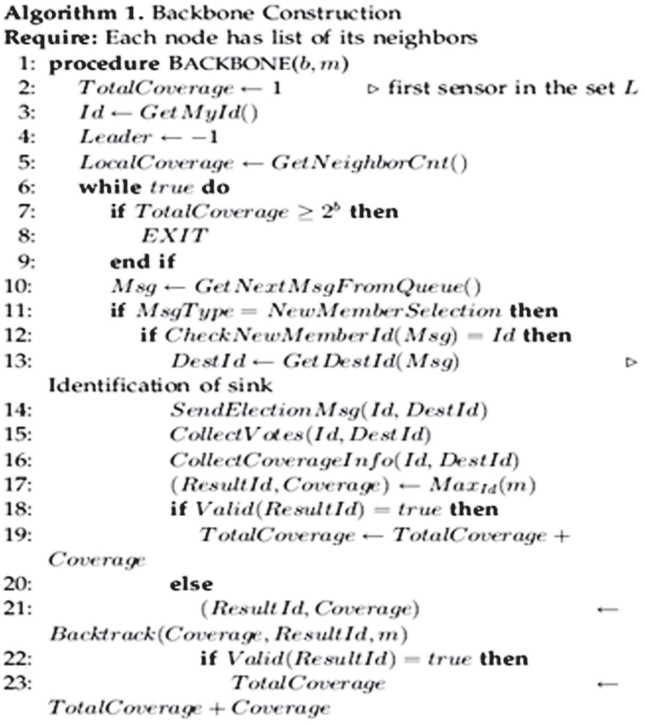
$$\omega_T=\sum_{i=1}^{\frac{T}{\alpha\times\Delta}}M_d(i)\times|S_A|,$$

Source Location Privacy Routing

Two techniques are used to protect location privacy of monitored objects. They are known as periodic collection and sourcesimulation. The former technique employs every sensor node to send packets periodically to deceive adversaries. Thus it can provide optimal privacy of location of monitored objects. However, it consumes more energy. In order to overcome this drawback source simulation technique is used. In this technique a set of fake objects are deployed in the field. Thus the adversaries will not be able to get the location details of real objects being monitored.

Sink Location Privacy Techniques

By finding sink locations, the adversaries can cause physical damage to sinks that disrupting the normal functionality of WSN. This can be avoided using two techniques known as sink simulation and backbone flooding. The former is used to fake sinks are simulate din the filed to deceive the adversaries. The latter is backbone flooding that sends packets to a connected portion of WSN instead of directly sending to sinks. The backbone is made up of some of the sensors. Thus the adversaries can't be able identify real sinks that and their physical locations. We have used algorithms proposed in [16] for backbone construction and also backtrack procedure.

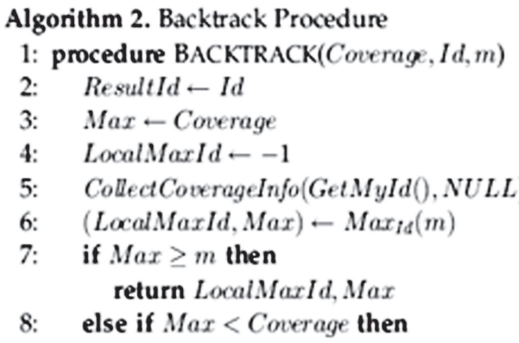


Algorithm 1. Backbone Construction

Require: Each node has list of its neighbors

```
procedure BACKBONE($(b, m)$)
    $TotalCoverage \leftarrow 1$                ▷ first sensor in the set $L$
    $Id \leftarrow GetMyId()$
    $Leader \leftarrow -1$
    $LocalCoverage \leftarrow GetNeighborCnt()$
    while $true$ do
        if $TotalCoverage \geq 2^b$ then
            $EXIT$
        end if
        $Msg \leftarrow GetNextMsgFromQueue()$
        if $MsgType = NewMemberSelection$ then
            if $CheckNewMemberId(Msg) = Id$ then
                $DestId \leftarrow GetDestId(Msg)$      ▷ Identification of sink
                $SendElectionMsg(Id, DestId)$
                $CollectVotes(Id, DestId)$
                $CollectCoverageInfo(Id, DestId)$
                $(ResultId, Coverage) \leftarrow Max_{Id}(m)$
                if $Valid(ResultId) = true$ then
                    $TotalCoverage \leftarrow TotalCoverage + Coverage$
                else
                    $(ResultId, Coverage) \leftarrow Backtrack(Coverage, ResultId, m)$
                    if $Valid(ResultId) = true$ then
                        $TotalCoverage \leftarrow TotalCoverage + Coverage$
```

Fig. 2 –Algorithm for Backbone Creation



Algorithm 2. Backtrack Procedure

```
procedure BACKTRACK($(Coverage, Id, m)$)
    $ResultId \leftarrow Id$
    $Max \leftarrow Coverage$
    $LocalMaxId \leftarrow -1$
    $CollectCoverageInfo(GetMyId(), NULL)$
    $(LocalMaxId, Max) \leftarrow Max_{Id}(m)$
    if $Max \geq m$ then
        return $LocalMaxId, Max$
    else if $Max < Coverage$ then
```

```
            $ResultId = LocalMaxId$
            $Max = Coverage$
        end if
        for $EachUnvisitedNeighborBKMember$ do
            $(Id, Coverage) = Backtrack(Max, ResultId, m)$
            if $Coverage \geq m$ then
                $ResultId = Id$
                $Max = Coverage$
                $break$
            else if $Coverage > Max$ then
                $Max = Coverage$
                $ResultId = Id$
            end if
        end for
          return $ResultId, Max$
    end procedure
```

Fig. 3 – Algorithm for Backtrack Procedure

As can be seen in figure 2 and 3, the algorithms are meant for protecting location privacy of sinks. Thus they can avoid the destruction of WSN by potential adversaries who are highly motivated. More technical details can be found in [16].

EXPERIMENTAL RESUTLS

Experiments are made using a prototype application built in Microsoft .NET platform. The platform provides environment to build applications. We built the prototype using C# programming language. The hardware environment used is a PC with 4GB RAM, core 2 dual processor running Windows 7 operating system. The experiments are made in terms of endangered animals in forest, privacy, communication cost, backbones, and fake base stations and so on. The results are presented as follows.

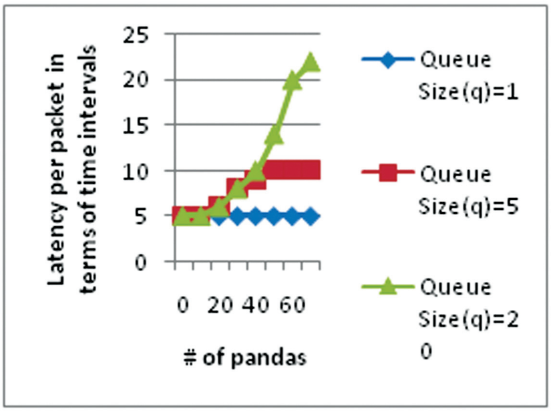


Fig. 4. Latency versus #pandas (periodic collection).

As shown in the above figure horizontal axis represents maximum of pandas while vertical axis represents latency per packet in terms of time intervals.

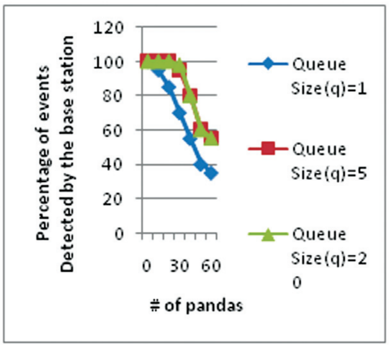


Fig. 5. Event detection versus #pandas (periodic collection).

As shown in the above figure horizontal axis represents maximum of pandas while vertical axis represents percentage of events detected by the base station.

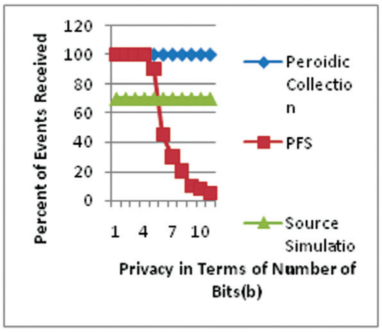


Fig. 6. Comparison of different source-location privacy schemes in terms of event detection rates.

As shown in the above figure horizontal axis represents percentage in terms of number of bits while vertical axis represents percent of events received.

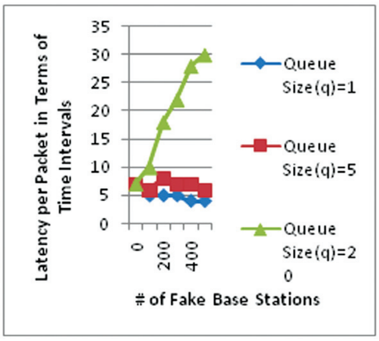


Fig. 7. Effect of the number of fake base stations on latency (sink simulation scheme).

As shown in the above figure horizontal axis represents maximum of fake base stations while vertical axis represents latency per packet in terms of time intervals.

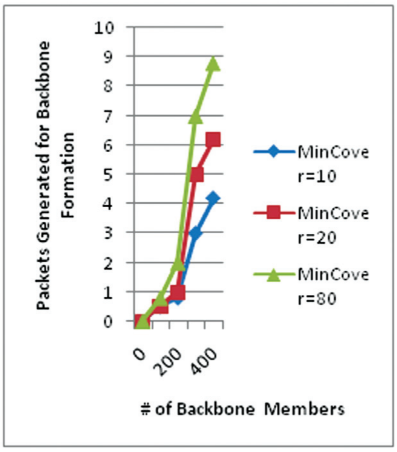


Fig. 8. Energy consumed for creation of backbone.

As shown in the above figure horizontal axis represents maximum of backbone members while vertical axis represents packet generated for backbone formation.

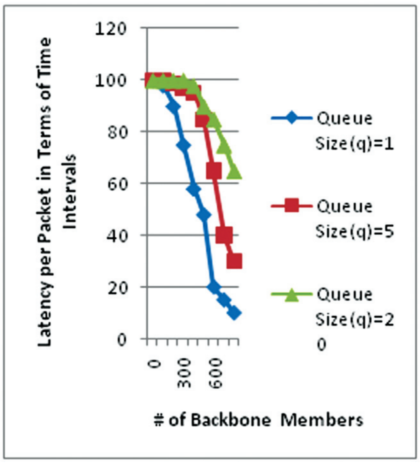


Fig. 9. Effect of the number of fake base station on the percentage of events detected by the base station (sink simulation scheme).

As shown in the above figure horizontal axis represents maximum of backbone members while vertical axis represents Latency per packet in terms of time intervals.

CONCLUSIONS AND FUTURE WORK

In this paper we explored location privacy against sink and monitored objects using a global eavesdropper model. The existing solutions focused on local eavesdropper which cannot withstand the attacks launched a more powerful global eavesdropper. We implemented techniques to ensure location privacy of monitored objects and sinks. Periodic collection and source simulation are the techniques used to provide location privacy to monitored objects while the sink simulation and backbone flooding are the techniques used to privde location privacy of sinks. We built a prototype application that demonstrates the proof of concept. The empirical results through simulations are encouraging. In future we will also consider global eavesdroppers compromising sensor nodes in the security model to provide location privacy of sensor nodes as well.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] 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.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. ACM MobiCom, July 2001.

[17] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE Int'l Conf. Network Protocols (ICNP '07), 2007.

[4] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.

[5] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008.

[6] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting Your Daily In-Home Activity Information from a Wireless Snooping Attack," Proc. Int'l Conf. Ubiquitous Computing (UbiComp '08), 2008.

[7] T.S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno, "Devices that Tell on You: Privacy Trends in Consumer Ubiquitous Computing," Proc. USENIX Security Symp., 2007.

[8] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.

[9] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.

[10] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "TowardsEvent Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.

[11] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.

[12] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.

[13] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

[14] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver- Location Privacy in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.

[15] Kiran Mehta, Donggang Liu and Matthew Wright, "Protecting Location Privacy in Sensor

Networks against a Global Eavesdropper". IEEE transactions on mobile computing, vol. 11, no. 2, february 2012.

AUTHOR

Sri Dr. BhaludraRaveendranadh Singh obtained M.Tech, Ph.D.(CSE)., is a young, decent, dynamic Renowned Educationist and Eminent Academician, has overall 21 years of teaching experience in different capacities. He is a life member of CSI, ISTE and also a member of IEEE (USA). For his credit he has more than 50 Research papers published in Inter National and National Journals. He has conducted various seminars, workshops and has participated several National Conferences and International Conferences. He has developed a passion towards building up of young Engineering Scholars and guided more than 500 Scholars at Under Graduate Level and Post Graduate Level. His meticulous planning and sound understanding of administrative issues made him a successful person.