International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 9 September 2015

Location Privacy Preserving Techniques in Wireless Sensor Networks against a Local and Global Eavesdropper

Ms. Harsha verma[1], Mr. Jitendra Dangra[2], Dr. M.K.Rawat[3]
M Tech Scholar[1], Asst. Professor[2], Head of Deptt.[3]
Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Indore-453331(M.P.), India
harshavermaa@gmail.com[1], jitendra.dangra@gmail.com[2], drmkrawat@gmail.com[3]

Abstract-*This paper presents the review of the various existing and recently proposed location privacy preserving techniques in wireless sensor networks (WSNs) against a local as well as global eavesdropper. Knowledge of the network topology in Local eavesdropper is limited while global eavesdropper can analyze the overall traffic pattern. Privacy preservation techniques are broadly classified into two categories 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. This survey paper compares the various privacy preserving techniques on the basis of parameters like efficiency, message overhead, power consumption, accuracy and delay.*

Keywords *- Sensor networks, location privacy, global eavesdropper.*

1. INTRODUCTION

A sensor network is an infrastructure that comprises number of wireless sensor nodes which consists of sensing, computing, communication, actuation, and power components that gives the ability to instrument, observe, and react to events and phenomena in a specified environment. The environment can be the physical world, a biological system, or an information technology (IT) framework. These networks are fundamentally different from traditional MANETs, where data is exchanged between any arbitrary pair of nodes. Sensor networks are based on "data centric" paradigms where, more than the specific nodes, the focus is on such attributes as temperature, motion, and region. Traditional routing protocols defined for MANET are not well suited for wireless sensor networks. The application-specific nature of these networks present unique challenges in the design of generic protocols at different layers of the network architecture.

Sensor networks have been used in the context of high-end applications like radiation and nuclear-threat detection system. Wireless sensor networks can be used in various applications includes military applications, environmental applications, health applications, home applications, and commercial applications. Existing and potential applications of sensor networks are military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, process control, inventory management, distributed robotics, weather sensing, environment monitoring, national border monitoring, and building and structures monitoring [1].For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable information or intelligence. Misuse of such type of information causes monetary loses or may also endanger human lives. Various researchers have focused considerable effort on finding ways to provide secrecy, integrity, attestation, and availability in sensor networks to protect such information. Though these are critical security requirements, they are insufficient in many applications. The patterns of communication in wireless sensors can, by themselves, reveal a great deal of contextual information, which can disclose the location information of critical components in a sensor network. For example, in military surveillance area where sensor network is deployed to command, control, communications, intelligence, and targeting systems. A global eavesdropper may analyze the traffic pattern and locate positions of the militants in the territory.

The communication architecture of a WSN is shown in Figure 1. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external base station(s). A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.

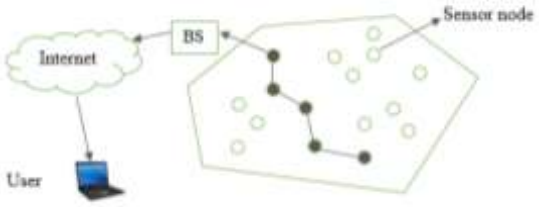

Figure: 1.Communication architecture of a WSN

2. PRIVACY IN WSNS

Privacy is the right to autonomy, and it includes the right to be let alone. Privacy encompasses the right to control information about ourselves, including the right to limit access to that information.

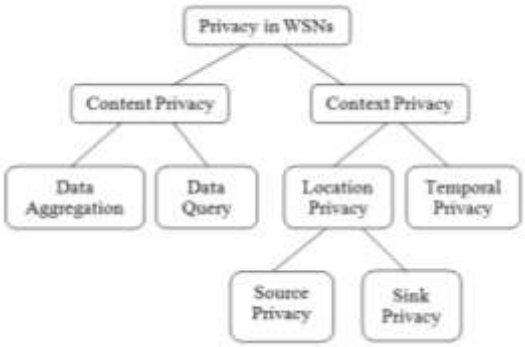

Figure: 2.Taxonomy of privacy preservation protection in WSNs

Privacy in WSN can be classified into two categories data oriented privacy and context oriented privacy as shown in Figure 2. 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. Content-oriented privacy is threatened by an adversary who aims to manipulate and/or read the content of messages sent over a WSN. Data-oriented protections are then categorized into privacy protections during data aggregation and private data query techniques. The main target of privacy protections is to privacy of data possessed by a network and queries posted to a network. There are two types of adversaries threatening the data privacy external adversary and internal adversary. The external adversary only eavesdrops communication in a network. This kind of adversary can be easily defeated by encryption techniques. However, an adversary unable to fetch the data contained in the packets can still bring back sensitive information by observing and analyzing the network traffic. Pai et al. [5] show that simple observation of network traffic may provide enough information about the data in which the network is dispose. Also there are some data aggregation protocols which reduce traffic of network by reusing the nodes forcedly in pass through packets to integrate their own sensed data, thereby increasing the size of packets as they reaches to the base station. Kamat et al. [4] says that both sensitive information and time taken of event are important, not only the occurrence of an event takes place i.e. temporal privacy. In the language of mobile asset monitoring, where an adversary can forebode the future behavior by linking the position and time of the events being monitored by the network.

3. Existing Privacy Preserving Routing Techniques

In this section, we provide overview of previously-proposed techniques and algorithms for source location privacy and sink privacy.

A. Source location privacy preserving techniques

Source location privacy mechanism prevents an attacker capable of performing traffic analysis attacks by determining the location of source node who reports the presence of an event in its territory. Source location problem was first described in the "Panda Hunter Scenario" [3,6] in which WSN is employed to monitor endangered pandas in their habitat. So privacy protection is needed at the data source.

Flooding technique [6] introduced by C. Ozturk, the source node sends out individual packet through various paths to the base station to make confusion for an adversary to trace the source. In baseline flooding mechanism whenever a sensor node detects an event it broadcast the corresponding message it to its neighbors. These neighbors also broadcast to their neighbor and finally multiple copies of the same

message being received by the base station through different nodes and thereby makes difficult for an adversary to detect the original source. The effectiveness of the baseline flooding depends on the number of nodes present on the transmitting path between the data source and base station. However, the issue is that the sink or base station will still receive packets from the shortest path first. By the failure of to provide enough privacy in return adversary can thus quickly trace the source node and this technique consumes a considerable amount of energy.

To overcome the problems faced in baseline flooding, probabilistic flooding technique is proposed in [6], in which each node has a preset probability of broadcasting the message. Due to probabilistic nature of node all nodes are not involved in forwarding the data which reduces the energy consumption. However, in this technique there is no guarantee that the base station receives the data send by the source due to the randomness involved.

The aim of the "random walk" is an approach in which bundle of data or packets select router and only through the network. In order to counter the adversaries, traffic analysis and forward traces, the path of packets should look completely random to an adversary. Solutions in this category use either a technique derived from the random walk, as described by Ozturk et al., or a technique that results in a similar pattern, such as rumor routing from Braginsky et al and routing through randomly selected intermediary node from Li et al.

Greedy random walk scheme proposed by Xi et al. for preserving location of a source node works in two phases. In the first phase, the base station will set up a path through random walk with a node that acts as a receptor. Then the source node will forward the packets towards the receptor in a random walk manner. Once the packet reaches the receptor, it will forward the packets to the sink node through the pre-established path. Here the receptor acts as an intermediary between the data source and sink for every communication session.

Geographic routing use the physical location of the nodes together with geographic routing algorithms to route packets through the WSN. In order to route a packet from the source to the sink, the geographic routing algorithms take the locality of a node, its neighbor's, and the sink into account. The approach in this section makes use of additional methods, such as the usage of synonyms, encryption, and random intermediary node selection to hide the flow of the traffic against a local adversary.

Another technique uses dummy data sources. In which we introduce dummy traffic to alter the real traffic. The motive is that an adversary should no longer be able to trace which part of the traffic is real, and which part is fake. In this category, we found the following solutions : aggregation-based source location protection scheme, a real and a fake cloud-based scheme for protecting source location privacy, constant rate , the dynamic bidirectional tree, distributed resource allocation algorithm, dummy wake-up scheme , fake sources 1 and fake sources 2, fitted probabilistic rate , the group algorithm for fake-traffic generation, globally optimal algorithm, the heuristic greedy algorithm, mixes, the optimal filtering scheme, periodic collection, persistent fake source routing, the probabilistic algorithm, proxy-based filtering, SECLOUD, short-lived fake source routing, source simulation, the timed efficient source privacy preservation, the timing analysis resilient protocol, tree based filtering ,the trusted computing enabled heterogeneous WSN , unobservable handoff trajectory , and the zigzag bidirectional tree.

Fake source mechanism [8] provides higher level of privacy. Base station creates the fake sources whenever a sender notifies the base station that it has real data to send. These fake senders are away from the real source and approximately at the same distance from the base station as the real sender. Both real and fake senders start generating packets at the same instance. This scheme provides decent privacy against a local eavesdropper. However, the power consumption in this mechanism is high.

Ozturk et al. [6] introduced a phantom routing scheme also called phantom flooding in which every packet send by the source node reaches the base station in two phases. In the first phase called walking phase in which the packets sent by data source travels in random manner within first h_{walk} hops. In the second phase the packets is flooded using the baseline flooding technique. In the first phase, the authors have introduced a bias in the random selection that makes it a directed random walk from a pure random walk to minimize the probability of creating routing loops. Because of the high path diversity the network size and intensity increases which improves source location privacy protection. However this technique may incur delays. For example, the packets may always expel from the base station because of a directed walk. Thus, this approach is not only well suited for the time sensitive applications. As we say the network size and the flooding phase is inversely proportional to the life time of the network.

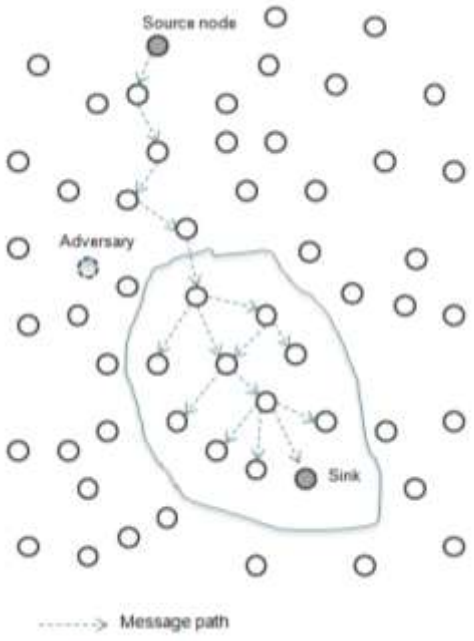

Figure: 3. Phantom Flooding

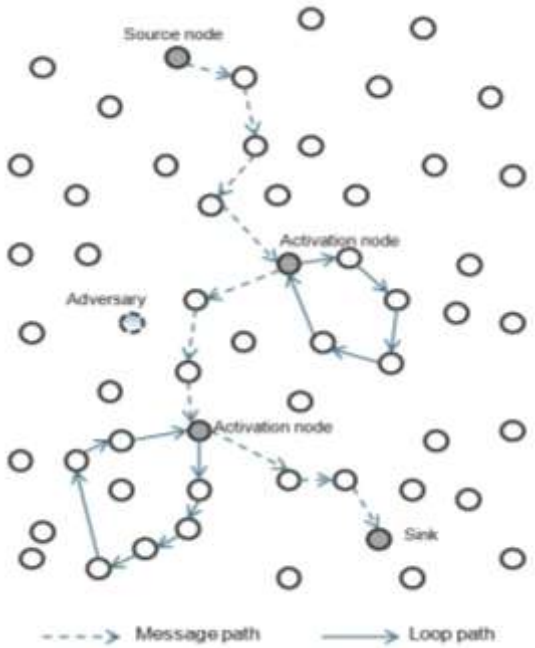

Figure: 4. Cyclic Entrapment

Phantom single-path routing proposed by Kamat et al. works in a similar manner as original phantom routing scheme discussed above. In this scheme, after the walking phase, the packets are to be forwarded to the sink via a single path routing strategy which provides less power consumption. However this scheme requires marginally higher memory as each node has to maintain routing tables. The drawback of this scheme is that it only provides protection against local adversary.

Cyclic entrapment method proposed by Ouyang et al. creates looping paths at various places in the sensor network as shown in Figure 4. This will cause a local adversary to follow these loops repeatedly and thereby increase the safety period which is defined as the number of messages initiated by the current source sensor before the monitored object is traced [7]. In this method, when the message is sent by the source node to the base station, it activates the pre-defined loops along the path. An activation node generates a fake message and forwards it towards the loop and original message is forwarded to the base station via specific routing protocol such as shortest path. Energy consumption and privacy provided by this method will increase as the length of the loops increase. The solutions in this category aim at confusing the adversary by shaping the traffic between nodes in cyclic patterns. A local adversary, who tracks the traffic between the nodes, will travel in circles without finding the actual source.

Mishra et al. proposed two schemes named Simple Anonymity Scheme and Cryptographic Anonymity Scheme for establishing anonymity in clustered WSNs. Simple Anonymity Scheme uses dynamic pseudonyms in place of a original identity during communications. Each sensor node has to store a given range of non-contiguous pseudonyms. So this scheme is not memory efficient. To overcome this problem the Cryptographic Anonymity Scheme uses keyed hash functions to generate pseudonyms. However, this mechanism is memory efficient but it requires more computational power and hence more power consumption.

A local adversary often needs multiple packets along the same route to track the actual source. The solutions based on separate path routing make sure that the packets travel via different nonintersecting paths from source to sink. Using separate paths leads to fewer packets per path, which delays the local adversary in its tracking, or even makes the adversary unable to track the actual source at all. This category consists of random parallel routing, weighted random stride routing, and weighted random stride routing towards a global viewing adversary.

B. Sink Location Privacy

Base station receives the entire data from the WSN, so location privacy is needed at the data sink. Consider the scenario of the military application. Figure 3 shows the WSNs deployed in the military surveillance area, where a

soldier 1 is sending confidential information to the soldier 2 i.e. sink via many intermediate nodes using multi-hop communication. A spy who is present on the same network tries to intercept the information by compromising one of the intermediate nodes. The nodes may reveal sensitive information to the adversary such location of the source or positions of the armed forces in the vicinity. Hence the protection of the base station is very important.

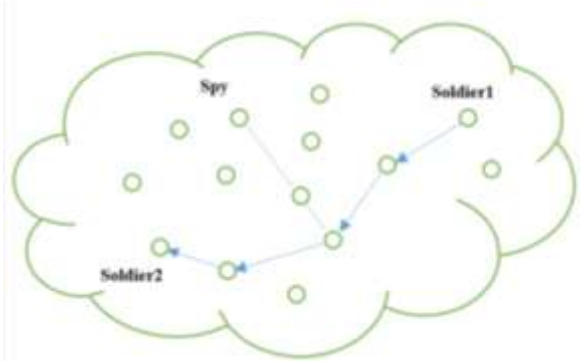

Figure: 4. Threats in military surveillance

An adversary has various techniques of traffic analysis and may attack the network. This includes the time correlation attack in which 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. By rate monitoring attack an adversary monitors the packet sending rate of the nodes and approaches to the nodes that have highest packet sending rate.

Higher level of privacy is achieved using hop by hop encryption technique in which the packets are re-encrypted hop by hop when it is transmitted to the sink. This technique hides the sink location through modifying the appearance of the data. However, even with hop by hop re-encrypted packets, an adversary can still deduce significant information that can reveal the sink location by monitoring traffic volume, or by time correlations.

Multiple parent routing scheme proposed by Deng et al. [9] reduces the starkness of pronounced paths caused by shortest path routing. In this pattern, when a node needs to forward a packet, the node randomly selects one of its parent nodes to forward the packet. This makes the patterns less pronounced in terms of routing packets towards the base station.

Controlled random walk technique [9] diversifies routing paths and mitigates rate monitoring attacks. In this scheme when a node receives a packet, it forwards the packet to one of its parent nodes with probability p_r. However; it uses a random forwarding algorithm with probability $1- p_r$. In the random forwarding algorithm, the node forwards the packet to one of its neighboring nodes with equal probability.

Fractal propagation technique addresses the shortcomings of multiple parent routing scheme and Random walk scheme. In this technique, numerous fake packets are generate and propagated in the network to enhance randomness in the communication pattern. When a node detects that its neighboring node is forwarding a packet to the base station, the node generates a fake packet with probability p_c, and forwards it to one of its neighboring nodes. This technique generates a large amount of traffic near the base station. This will potentially increase the packet collision rate and packet loss rate.

Differential fractal propagation technique [9] addresses the problem faced in simple propagation. In this technique, nodes can use different probabilities to generate fake packets. When a node forwards packets more frequently, it sets a lower probability for creating new fake packets.

In Differential Enforced fractal propagation [9] technique local high data sending rate areas called hot spots are generated in the network. An adversary may be trapped in those areas and not be able to determine the correct path to the base station.

4. COMPARISON

There are several ways by which an adversary can trace the location of receiver. First, by analyzing the traffic rate an adversary can deduce the location of the receiver. Basic idea behind traffic-analysis attack is that sensors near the receiver forward a greater volume of packets than sensors further away from the receiver [2]. First, an adversary is able to compute the traffic densities at various locations by eavesdropping the packets transmitted at these locations in a sensor network, based on the analyzed result it deduces the location of or the direction to the receiver. However, to perform the traffic-rate analysis, an adversary has to stay at each location long enough such that sufficient data can be gathered for computing the traffic rate. This process takes a long time as the adversary moves from location to location. Second, an adversary can reach the receiver and determines the original source by following the movement of packets. This packet-tracing attack [3], breach the privacy of the sender's location. In this attack, an equipped adversary can easily find the location of the immediate transmitter of an overheard packet, and through this information he is able to perform hop-by-hop trace towards the original source.

Table 1: Comparison of location privacy techniques for the data source and sink against local eavesdropper

Techniques	***Location***	***Adversary***	***Comparison Summary***
Baseline flooding	Data Source	Local adversary	**Efficiency** - Not efficient as effectiveness depends on the number of nodes present on the transmission path between the data source and base station. **Power Consumption** - High due to flooding of data in network **Accuracy** - Guaranteed data arrival at sink.
Probabilistic flooding	Data Source	Local adversary	**Efficiency** - Efficiency equivalent to baseline flooding. **Power Consumption** - Low compared to baseline flooding due to less nodes involved in flooding **Accuracy** - No guarantee of data arrival at sink.
Phantom flooding / Phantom routing	Data Source	Local adversary	**Efficiency** - Much more efficient then baseline and probabilistic flooding technique. **Power Consumption** - High **Accuracy** - Guaranteed data arrival at sink.
Phantom single-path routing	Data Source	Local adversary	**Efficiency** - Efficiency equivalent to phantom flooding. **Power Consumption** - Low compared to phantom flooding. **Accuracy** - Guaranteed data arrival at sink.
Cyclic entrapment	Data Source	Local adversary	**Efficiency** - More efficient then above techniques. **Power Consumption** - High ; Power consumption increases when length of loop increases. **Accuracy** - Guaranteed data arrival at sink.
Simple Anonymity Scheme	Data Source	Local adversary	**Efficiency**– High **Power Consumption** - Medium **Accuracy** - Guaranteed data arrival at sink.
Cryptographic Anonymity Scheme	Data Source	Local adversary	**Efficiency**– High **Power Consumption** - More than simple anonymity scheme. **Accuracy** - Guaranteed data arrival at sink.
Greedy Walk	Data Source	Local adversary	**Efficiency** - Highly efficient **Power Consumption** - Medium **Accuracy** - Guaranteed data arrival at sink.
Fake Sources	Data Source	Local	**Efficiency** - Highly efficient

		adversary	**Power Consumption** - High **Accuracy** - Guaranteed data arrival at sink.
Hop by hop encryption	Base station	Local adversary	**Efficiency** - Highly efficient. **Power Consumption** - Medium. **Accuracy** - Guaranteed data arrival at sink.
Multi-Parent Routing	Base station	Local adversary	**Efficiency** - Efficient. **Power Consumption** - Medium **Accuracy** - No guarantee of data arrival at sink.
Controlled Random Walk	Base station	Local adversary	**Efficiency** - Efficient. **Power Consumption** - Medium **Accuracy** - No guarantee of data arrival at sink.
Fractal propagation	Base station	Local adversary	**Efficiency** - More efficient than multi-parent routing and controlled random walk. **Power Consumption** - Medium **Accuracy** - No guarantee of data arrival at sink.
Differential Fractal Propagation	Base station	Local adversary	**Efficiency** - Highly efficient. **Power Consumption** - High. **Accuracy** - No guarantee of data arrival at sink.
Differential Enforced Fractal Propagation	Base station	Local adversary	**Efficiency** - Highly efficient **Power Consumption** - High **Accuracy** - No guarantee of data arrival at sink.

VI. Conclusion

This paper presents the comparison of various location privacy preservation techniques. Comparison parameters include efficiency, adversary (local or global), message overhead, power consumption, accuracy and delay. On the basis of comparison and analysis of all the existing privacy preservation techniques it has been concluded that against a local eavesdropper we can achieve the location privacy while against a global eavesdropper the proposed techniques have much communication overhead. In future, techniques are required which provides location privacy with reduced communication overhead and power consumption against a global eavesdropper.

References

[1] T. Znati, C. Raghavendra and K. Sivalingam, Guest editorial, Special Issue on Wireless Sensor Networks, Mobile Networks and Applications, Vol. 8, No. 4, Aug. 2003.

[2] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," Proc. of CerateNet Conference on Security and Privacy in Communication Networks(SecureComm), 2005.

[3] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor

network routing," Proc. of 25th IEEE Inter-national Conference on Distributed Computing Systems (ICDCS), 2005.

[4] P. Kamat, W. Xu, W. Trappe, and Y. Zhang. Temporal Privacy in Wireless Sensor Networks. In ICDCS '07: Proceedings of the 27th International Conference on Distributed Computing Systems, page 23, Washington, DC, USA, 2007. IEEE Computer Society.

[5] S. Pai, S. Bermudez, S. Wicker, M. Meingast, T. Roosta, S. Sastry, and D. Mulligan. Transactional Confidentiality in Sensor Networks. IEEE Security & Privacy, 6(4):28–35, July-Aug. 2008.

[6] 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 ad hoc and sensor networks (SASN), pages 88–93, October 2004.

[7] 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.

[8] 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.

[9] J. Deng, R. Han, and S. Mishra. "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks". Elsevier Pervasive and Mobile Computing Journal, 2:159–186, April 2006

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

[11] Yi OuyangZhengyi Le, Guanling Chen, James Ford, and FilliaMakedon.,"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] Y. Xi, L. Schwiebert, and 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.

[13] 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.

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