International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Protecting Location Privacy in Wireless Sensor Networks against Eavesdropper

Seema Goswami
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Nidhi Chandrakar
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Somesh Dewangan
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

***Abstract*— A result of the wireless characteristics of communication in sensor network, the communication patterns involving sensors could possibly be leaked whatever the adoption associated with encryption mechanisms—those might just protect the message content. Nevertheless, communication behaviour could offer valuable information for an adversary. For example, this will be the case whenever sensors reply to a problem broadcast with a Base Station (BS); an adversary eavesdropping the particular communication visitors could understand which detectors are those who possibly fit the query This trouble is complicated from the severe learning resource constrained environment WSNs are governed by, that call for efficient along with scalable remedies. Even though a great deal security is given from the wireless sensor networks the information has been exposed. Such information may then used from the adversary to the attack. The prevailing privacy techniques reduce the chances of a neighborhood adversary. You will discover two main types of privacy preservation in Cellular Sensor Networks. They are data privacy plus the context level of privacy. Existing approaches defend the particular leakage associated with location information from your limited adversary who is able to only view network traffic inside a small place. However, any stronger adversary, the international eavesdropper, is realistic which enables it to defeat these kind of existing approaches. This cardstock first formalizes the place privacy difficulties in sensor sites under that strong adversary model along with computes a lesser bound on the communication overhead required for achieving settled level associated with location privacy.**

Keywords—Wireless Sensor Networks, Privacy, location privacy, Eavesdropper, Probabilistic algorithm, Resiliency, Security.

I. INTRODUCTION

An wireless sensor network (WSN) is created of the sensor nodes. These nodes changes from few to hundreds a number of thousands. Sensors are capably of monitoring the physical place, temperature, vibration, seem, etc along with send for the base section. The sensor nodes are inclined to failures this can be due for the battery, over head, environment etc. A large amount of work continues to be done to boost the performance from the power along with resources utilizing different direction-finding algorithms however these days there is need from the privacy from the individuals.

Wireless sensor network describes a group of spatially spread and focused sensors with regard to monitoring along with recording the physical conditions from the environment along with organizing the collected data in a central place. The primary characteristics of wireless sensor network include:

- Power consumption constrains with regard to nodes utilizing

batteries or even energy harvesting
- Ability to deal with node downfalls
- Mobility of nodes
- Communication downfalls
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand unpleasant environmental problems
- Ease of usage

Sensor networks can be employed for wide variety of applications where it really is difficult or even infeasible to setup wired sites. Some from the areas contain forest fireplace detection, air pollution monitoring, wellness, wildlife home monitoring etc. A sensor network may be deployed in a very forest to detect the occurrence of fire. Your sensors calculate the temp, humidity along with gases due to the fire inside trees or even vegetation. Wireless sensor networks happen to be deployed in a variety of cities to detect unusual chemical agents inside air. Sensors are widely-used by the doctors to monitor the physiological condition of affected individual. Privacy is just about the most significant problems within wireless sensor networks due to the open nature of instant communication, rendering it very possible for adversaries to eavesdrop. Privacy in sensor sites is divided into 2 categories: written content privacy, which concerns with all the content of data packets, along with transactional solitude, which is targeted on information about the traffic attributes (such seeing that carrier volume, message charge and routing). Although written content privacy may be protected by means

of strong encryption along with authentication parts, sensor networks endure malicious visitors analysis.
The complete lifetime of an wireless sensor network may be divided in to two varieties of operational stages: topology development and data transmission.

II. Background and Related Works

location privacy possesses gained a lot more attentions. According to the difference connected with objects protected, previous studies can be divided in two kinds: preserving source location solitude and safeguarding sink position privacy. The main element idea connected with protection is always to confuse your adversary as well as conceal the important location connected with BS in redundant bogus information, including fabricating bogus sources/sink randomly walk as well as fake packet injection.
Kamat et 's. designed some sort of routing process called Phantom routing to protect the location privacy connected with source nodes. With Phantom routing, packets randomly walk into a virtual source before the normal delivery. However, Phantom routing cannot protect your receiver's position privacy properly. Additionally, randomly walk prolongs your delivery latency.
Deng et 's. proposed Differential Forced Fractal Propagation (DEFP) versus traffic evaluation attack for the location privecy of BS. Multi-path direction-finding and bogus message propagation are released into DEFP. But this specific work concentrates on the traffic-analysis strike, which is not a more suitable measure to have an adversary.
Jian et 's. designed the location privacy direction-finding protocol (LPR) to protect the receiver's location]. LPR combines both randomly walk as well as fake packet injection. On the other hand, random stroll brings more packet hold up, and bogus packet injection in LPR is completely random, with no consideration connected with optimization matter.
Deng et 's. address the challenge of the best way to hide the location of the bottom station within a sensor network. Techniques connected with multi-path direction-finding and bogus message injection are released. However, the effort concentrates for the traffic-analysis strike, which determines the bottom station's location through the measurement connected with traffic charges at different locations. We have remarked that the traffic-analysis strike takes for a longer time time to identify a receiver compared to packet-tracing strike. The simulation ends up with Section Versus will demonstrate how the method won't perform properly in defending against the packet searching for.
Deng et 's. propose another way of protecting the bottom station versus traffic-rate evaluation attacks. The transmission times from the packets are generally randomly delayed so that you can hide your traffic pattern plus the parent-child relationship under a clear traffic pace model. However, this strategy introduces more delay pertaining to delivering packets within a sensor network.
Nezhad et 's. considered your privacy problem throughout the topology discovery period as well as proposed an distributed strategy for network topology discovery to protect the destroy location solitude. However, this process has a higher complexity as well as brings more load in order to sensor communities.
Privacy matter is widely explored in the field of database, communities, data mining and also other field. Plenty of techniques are generally proposed pertaining to privacy preservation including: Cryptographic protection, K-anonymity. These methods are use to protect data whenever it flows in one node in order to other your figure 1 demonstrates the distinction of solitude preservation troubles in wi-fi sensor network We, thus, focus upon privacy preserving techniques created to defend versus a wide-spread eavesdropper.
Kamat et 's. designed some sort of routing process called Phantom routing to protect the position privacy connected with source nodes [5]. With Phantom direction-finding, packets randomly walk into a virtual source before the normal delivery. However, Phantom routing cannot protect your receiver's position privacy properly. Additionally, randomly walk prolongs your delivery latency.

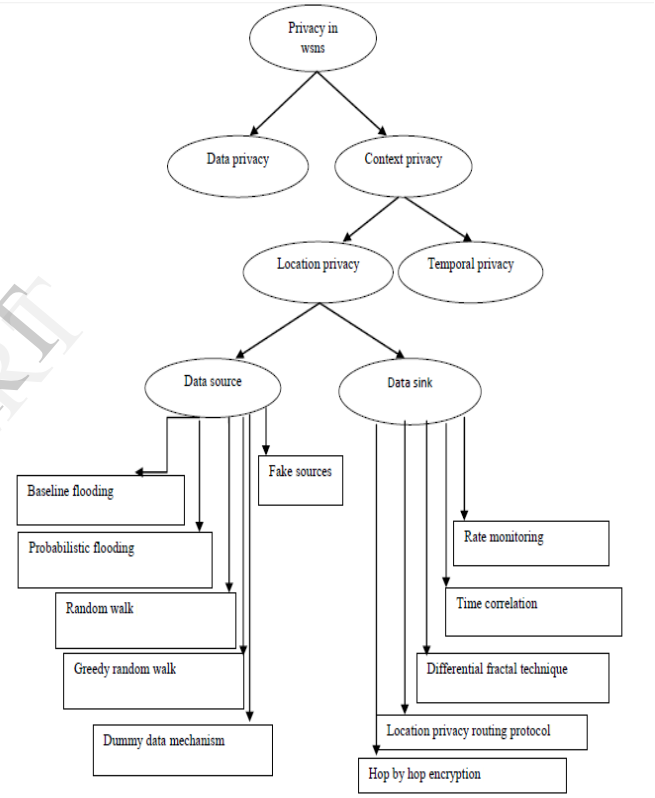

Figure 1 Classification of the privacy preserving problems for WSN.

III. System Model and Preliminary

A. Network Model

an wireless sensor network consists of a Base Section (BS) and a large number of common sensors. Each sensor, comparatively stationary, provides the same radio selection of r. work with a connected graph G(V, E) in order to represent your wireless sensor multilevel. Every individual sensor (including BS) is an element of V, and every communication url is denoted by a good sharp edge in E. Vs represents the pair of source nodes. A great arbitrary node t maintains the neighbor list N(t), recording individuals nodes that talk with t.

B. Communication Model

There are mainly two varieties of operational phases of the wireless sensor network: topology breakthrough and information transmission. Over the topology breakthrough period, BS broadcasts some text that contains an incremental ut value, to ensure every node is aware the minimal routing distance from BS. Inside data transmitting period, origin nodes routinely transmit sensed information to BULL CRAP through a number of hops, and the time is described as Delivery Period (Tp). We use Speediest Path Routing (SPR) seeing that our simple routing method, in which every node forwards packets towards neighbors who have a smaller sized hop value. Note how the time span of topology breakthrough period is actually longer than that regarding topology transmitting period seeing that shown with Fig. 1. Periodical topology discovery is important. The reason is how the global topology might have changed because of the mobility or absence of individual nodes, age. g. some nodes digest or go out of battery.

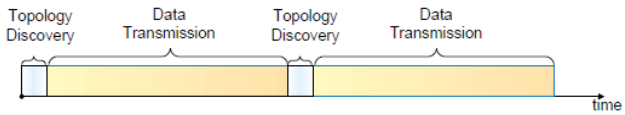

Figure 2 Different operational phases of the WSN

In addition, data aggregation method, in which sensor node aggregates numerous received packets to 1 packet. For example, the purpose of data selection is to discover the average importance of found values (e. gary the gadget guy., the conditions in a area), so because of this nodes is able to do in-network processing. After obtaining several data packets, sensor node for starters calculates the typical value and then delivers this spark a new data packet. Therefore, we assume that every packet transmitted in sensor networks has got the same size to be able to prevent the actual adversary through inferring the venue of BS in line with the packet dimensions.

C. Adversary Model

The adversary provides the following features:

Non-malicious: The objective of the adversary would be to capture BS, which indicates the adversary isn't going to interfere your communication involving sensor communities, otherwise a great intrusion diagnosis system might discover his / her malicious steps.

Device-rich: The attacker is containing more devices: endless power, memory space and working out capability. The guy can estimate the place of any sender node over the analysis on the arrival angle and indicate strength. Specifically, we believe the adversary has a fixed overhearing range R, which can be greater compared to radio variety of sensors, 3rd there s r.

Policy-informed: The attacker is informed about the protection method. He can find BS visually when he could be close enough to it.

Content-unaware: The attacker cannot find the content involving data packets, which can be guaranteed by simply underlying encryption.

Speed-limited: The movement on the adversary will be far slower compared to packet, which means in any delivery period of time Tp, the guy can only take notice of the delivery path inside the overhearing range R but is not the total path. Like a smart attacker, he practices these invasion policies:

• He or she either chooses to visit a package or stays for a node to help overhear more packets.

• He or she records the last path which he has visited, and backtracks whenever necessary.

IV. EXISTING APPROACHES

A large numbers of attacks are possible in WSN such as Denial of Service attacks, The Sybil attacks, Traffic Analysis attacks, attacks against Privacy, and Physical attacks. Lot of work has done to overcome these attacks .Our area of interest is on attacks against Privacy. Privacy attacks can be further classified into two broad categories data oriented attacks and context oriented attacks. The following are the different existing techniques for the location privacy preservation against a eavesdropper.

A. *Flooding*

Flooding have been used in order to preserve the particular physical location on the data supply. In the way it is of the particular baseline water damage mechanism. a sensor node picks up the presence on the panda and broadcasts it to their neighbors. These neighbors therefore broadcast on their neighbor and finally being received by the base train station. The rogue notices which the base train station.

B. *Probabilistic flooding*

To deal with the result of the baseline inundating, probabilistic inundating is recommended, in this mechanism not every sensors initiate the forwarding info rather just about every node broadcasts with a Preset possibility. This system reduces the energy consumption but there isn't any guarantee of the reception data with the base station as a result of randomness involved this process.

C. *Random Walk Mechanism*

More impressive range of privacy is possible through the arbitrary walk process where within phantom routing is utilized. In this kind of a arbitrary walk is completed from the results source, and a probabilistic inundating scheme is actually then applied. fig 3.Exhibits the arbitrary walk process.

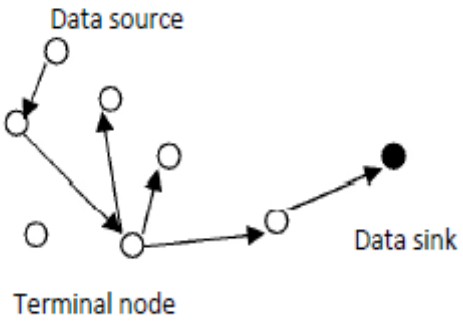

Figure 3 Random walk mechanism

D. *Greedy Walk Mechanism*

Another higher-level technique would be the greedy random walk where from the base train station first initializes some sort of random path which has a given variety of the hops. Sensors with this particular way are called the receptors. Then some sort of packet is randomly forwarded from your data supply until many people reach on the list of receptors. Thereby then pursuing the pre recognized path by the base train station. Fig several. Shows the actual greedy wander mechanism. To help protect the actual physical location of the data supply dummy info mechanism is employed. In this specific fake packets usually are introduced to be able to disturb the actual traffic. an effective scheme of the short existed fake supply routing is proposed where in just about every sensor transmits a fake packet which has a pre identified probability. Upon finding a fake packet, a sensor node only discards the actual packet in addition to upon receiving the genuine packet that forward on the base train station. However strength efficiency is maintained but along the just about every path for the fake way is a single hop. Meaning that the hunter as well as the attacker can throw away the fake paths in addition to reach on the physical location of is provided with multiple copies of the same message. And there by perplexing the hunter or the actual adversary. However the potency of the base lining flooding is determined by the not any of nodes on the transmission path between your data supply and base station. When the path is too short then this hunter will use the least path between your data supply and base station.

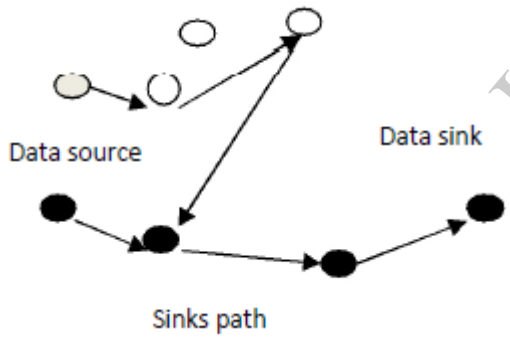

Figure 4 Greedy walk mechanisms

E. *Fake Sources Mechanism*

The still advanced of privacy is achieved with the help of the phony sources procedure. In this kind of mechanism a number sensor nodes tend to be chosen in order to simulate the behavior in the real data source in order to confuse the adversary. however power consumption is reasonably high..

F. *Proxy based filtering*

The fundamental idea involving PFS is which a compartment involving sensors inside the network will probably be selected because proxies to collect and decline dummy communications before they will reach the base station so your problem involving high conversation cost involving interrupted bundle transmission is mitigated. If among the incoming packets to your proxy corresponds to your real celebration, proxy's outgoing bundle carries in which information; otherwise the outgoing packet is usually a dummy just one. In one more view, a proxy acts as being a base place, it gathers packets from other devices but since it doesn't have an immediate connection towards outside earth, the data it collects need to be sent towards base place again in the periodic trend to sustain privacy components. Hence the results is hidden in the controlled fashion with an outsider making sure that any useful information can not be extracted on the traffic patterns affecting the system data movement (i. age., a worldwide eavesdropper can't determine whether or not an event-triggered activity is occurring in the network and cannot select any specific node because the source node).

G. *Tree based filtering*

TFS, your second scheme, makes it possible for filtering at multiple proxies. Inside TFS, proxies form a tree rooted structure in the base section with each and every proxy developing a parent node and perhaps multiple baby nodes. Parent nodes next aggregate visitors originated by child nodes and also child leaf nodes combination data received from ordinary receptors.

H. *Periodic Collection*

With periodic collection method possesses every sensor node individually and periodically send packets in a reasonable frequency no matter if there is real info to post or not.

I. *Source simulation*

Everybody will generate a visitors pattern similar to that of your real object. After network deployment, each digital object can be treated just like a real object, as detectors detect the item and send the object's information towards destination. The particular protocol works in times. In every single round, the node simulating the actual false object will randomly look for a sensor node throughout its local community (including itself) and enquire this node to simulate the true object next round..

V. PROBLEM DEFFINETION

Inside previous exploration and research, there assume how the global eavesdropper does not compromise sensor nodes. Even so, in process, the world-wide Eavesdropper may be able to compromise a subset on the sensor nodes from the field and also perform site visitors analysis along with additional expertise from insiders. This specific presents useful challenges for you to methods. But it takes time to the observations made by the adversarial network to succeed in the enemy for analysis and response. Studying the impact connected with such “delayed” analysis and reaction will be another useful research course. and the vast majority of techniques add more energy consumption.

VI. PRAPOSED WORK

Much like this analyze we identify some dilemma in problem identification area and that is present within the almost all of the previous methodologies. The major objectives to operate on that area should be to develop a much better techniques when it comes to location privacy against global eavesdropper, energy intake and time taking on the observations of the adversarial network to achieve the foe for evaluation and

response. We will certainly prapose any enhanced strategy in expression of Better location privacy against eavesdropper using less power consumption and less time come to to the observations of the adversarial network to achieve the foe for evaluation and response.

ACKNOWLADGEMENT

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on Location Privacy in Wireless Sensor Networks. I sincerely express my gratitude to Mrs. Nidhi chandrakar of Dept. of M.Tech CSE, DIMAT for giving constant inspiration for this work. I am also thankful to Mrs. Preeti Tuli, Prof. Somesh Dewangan, Dept. of CSE, DIMAT for helping me directly and indirectly during this work. I am really thankful to my all friends for their blessing and support.

REFFERENCE

[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] 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.
[3] BlueRadios Inc., "Order and Price Info," http://www.blueradios. com/orderinfo.htm, Feb. 2006.
[4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree," Combinatorica, vol. 24, no. 2, pp. 187-207, 2004.
[5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.
[6] 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.
[7] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '04), June 2004.
[8] 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.
[9] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '02), Nov. 2002.
[10] 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.
[11] H. Gupta, Z. Zhou, S. Das, and Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," IEEE/ACM Trans. Networking, vol. 14, no. 1, pp. 55- 67, Feb. 2006.
[12] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy, "The Platforms Enabling Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 41-46, 2004.
[13] 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.
[14] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet draft, Feb. 2002.
[15] 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.
[16] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003.
[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.
[18] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) Using AoA," Proc. IEEE INFOCOM, pp. 1734-1743, Apr. 2003.
[19] 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.
[20] 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.
[21] V. Paruchuri, A. Duressi, M. Duressi, and L. Barolli, "Routing through Backbone Structures in Sensor Networks," Proc. 11th Int'l Conf. Parallel and Distributed Systems (ICPADS '05), 2005.
[22] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad Hoc On- Demand Distance Vector (AODV) Routing," IETF Internet draft, Feb. 2003.
[23] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. ACM MobiCom, July 2001.
[24] 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.
[25] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," Proc. ACM MobiCom, July 2001.
[26] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.
[27] 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.
[28] H. Takahashi and A. Matsuyama, "An Approximate Solution for the Steiner Problem in Graphs," Math. Japonica, vol. 24, pp. 573- 577, 1980.
[29] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.
[30] K. Sohraby, D. Minoli and T. Znati. , "W ireless Sensor Netwo rk: Technology, Protocols and Applications:", John Wiley & Sons, 2007,pg10-11.
[31] C. Ozturk, Y. Z hang, and W. Trappe. "Source-l ocation privacy in e nergy constrai ned sensor network routing": In Proceedings of the 2nd ACM workshop on Security of Adhoc and Senso r Networks, 2004
[32] R. Agrawal, A. Evfimievski, R. Srikant,, "Information sharing across private databases in:" : Proceedings of the 2003 ACM SIGMOD International Confere nce on Management of Data, 2003, pp. 86–97.
[33] L. Sweeney, " K-anonymity: a model for pro tecting privacy, Inter national Journ al on Uncertainty, Fuzziness and K nowledge based Systems" 2 (2) (2002) 557–570. pp. 86– 97.
[34] Na Li, Nan Z hang, Sajal K . Das, and B havani Thuraisingham, " Privacy pre servation in w ireless sensor networks : A state-of-th e-art survey". A d Hoc Networks 7 (20 09) 1501–1514.
[35] Jean-Franois Ra ymond. Traffi c analysis: Pro tocols, attacks, design issues and open proble ms. In Proceedings of International Workshop on Design Issues in Anony mity and Unob servability, pag es 10- 29. Springer- V erlag New York, Inc., 2001.
[36] Celal Ozturk, Yanyong Zhan g, and Wade Trappe, "Source locatio n privacy in energy-constrained sensor network routing ". In SASN '04: Proceedings of the 2nd ACM works hop on Securit y of ad hoc and sensor networks, pages 88-93, New Y ork, NY, USA, 2004. ACM.
[37] Y. Xi, L. Sch wiebert, W.S. S hi, 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.
[38] 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
[39] 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.
[40] 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.

[41] 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.

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