Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.4, No.3, 2014

www.iiste.org

A Review of Privacy Preserving Techniques in Wireless Sensor Network

Snehal M. Gaikwad[1*] Vidya Dhamdhere[2]

1. M.E. student, G.H.Raisoni College of Engg. And Mgmt.,Pune,Maharashtra,India
2. Asst. Prof. , G.H.Raisoni College of Engg. And Mgmt.,Pune,Maharashtra,India

* E-mail of the corresponding author: gaikwad.snehal99@gmail.com

Abstract

This paper represents a review of privacy preserving techniques in wireless sensor network. Wireless sensor networks are not secure. To preserve privacy of wireless sensor network various techniques are discovered. A lot of work has been done to address challenges faced to preserve privacy of wireless sensor network. In this paper we represent a research on privacy preserving techniques used in location privacy, data privacy and network privacy. This paper should provide help for further research in privacy preservation in wireless sensor network.

Keywords: Context privacy, data privacy, source location privacy

1. Introduction

1.1 Wireless sensor network and its applications:

Fig.1. shows architecture of wireless sensor network. A wireless sensor network [1] is a collection of sensor nodes which has resource limitations such as battery power, storage and communication capability. This collection of sensor nodes uses radio interface to communicate with one another to form a network. Simple equation of wireless sensor network is sensing power+processor+radio=possible applications.

Wireless sensor network has many important and necessary applications [25]. Wireless sensor network can be Terrestrial Wireless sensor network, Underground Wireless sensor network, Underwater Wireless sensor network, Multi-media Wireless sensor network, Mobile Wireless sensor network. These sensor networks are used in many applications like security, monitoring, biomedical research, tracking etc.

These applications are divided into many classes like Environmental Military applications, data collection, Security monitoring, Wildfire detection, sensor node tracking, health application, home application, and hybrid networks. At the beginning wireless sensor network was used in defense application like in military. VigilNet is a wireless sensor network used in military that captures and verifies information about enemy capabilities and positions of hostile targets. Wireless sensor network is also used in environmental data collection operation used to collect various sensor data in a particular period of time. In disaster relief operation also wireless sensor network is used in wildlife detection by dropping sensor nodes from aircraft over wildlife. Wireless sensor network is used in facility management for intrusion detection into industrial sites and other restricted areas. Most important use of wireless sensor network is in medical and healthcare for post-operative or intensive care of patient. Wireless sensor network is also used in vehicle telemetries by providing better traffic control by obtaining finer-grained information about traffic conditions. WSN is also used in home applications like TV, air conditioner.

WSN offers a wide variety of applications[27] that can be implemented in real world. But to implement them a lot of challenges need to be addressed. These challenges are :Types of Service, QOS, Fault tolerance, Lifetime, Scalability, Wide range of densities, Programmability, Maintainability, Multihop wireless communication, Energy-efficient operation, Auto-configuration, Collaboration and in-network processing, Data-centric networking, Locality, Exploit trade-offs, privacy.

a. Types of service: Wireless sensor network does not mean simply transferring or moving information from – Not simply moving bits from one place in the network to another rather it needs to move meaningful information. For example moving information through WSN in given time interval or in specified geometrical region only.

b. Quality of Service (QOS): Maintain QOS in application like multi-media or time critical Multi-media application requires enough good quality of contents (video, audio and image). In time critical application, the data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless.

c. Fault tolerance: Sensor nodes are prone to failure because of unattended environment. Hence we need to provide new protocol, algorithms to handle these types of failures.

d. Lifetime: Lifetime of sensing node.

e. Scalability: Architecture and protocols of WSN need to support a large number of sensors.

e. Programmability: Increase the flexibility by enabling the re-programming of nodes in the field to react to new situations

f. Maintainability: Maintenance of WSN nodes and other devices over changing requirements.
g. Security: An effective and efficient compromise should be achieved, between security demands for secure communication and low bandwidth required for communication in sensor network.

1.2 Need for preserving privacy in WSN application[27]

Privacy issue is widely explored in the field of database, networks, data mining and other fields. Many techniques are used to protect data when it flows from one node to other. Fig.2 shows privacy types [26] in wireless sensor network. There are many attacks against the privacy. These privacy Attacks are classified into two main categories and this shows why privacy preservation is very needful in WSN. Categories are a. Data oriented privacy and b. Context oriented privacy.

1.2.1. Data Oriented privacy mainly deals with preserving privacy of data which is collected from different nodes and sent to the sink node known as data aggregation because attacker is trying to get or modify the data which is transferred between source and sink node and solve privacy problem of data query.
1.2.2. Context oriented privacy deals with protection of sensor event because sensor events are so sensitive that it is needed to protect all information surrounding these sensor events. The context-oriented information includes information on source location, sink location and timing of events.
1.2.2.1. Location privacy: Location privacy plays an important role in WSN such as, location of special sensor node, data source. Adversary can find out location of sensor node that monitors the important object, successfully localizes and captures the object.
1.2.2.2. Temporal privacy: Temporal privacy is important in the mobile target tracking application of WSN. For example in military field where assets are sensed by a sensor node an adversary with knowledge of such timing information may be able to predict the moving path of the mobile target in the future, thus violating the privacy of the target.

1.3 Need for research on preserving privacy in WSN

Section 1.2 describes privacy categories in wireless sensor network. There are many attacks against the privacy categories. Many techniques have been discovered for preserving privacy of data as well as location. But to increase security and privacy of data more research needs to be done on privacy preservation. Only a few people have carried out a research on attacks on privacy of data which is stored at sink. Therefore more research needs to be done in this area.

1.4 Challenges in privacy preservation WSN [25]

Privacy protection has been important in many fields like wireless networking, databases and data mining. The following features of WSNs introduce unique challenges for privacy preservation of data and prevent the existing techniques from being directly implemented in these networks.

1.4.1 Uncontrollable environment: sensors may have to be deployed in an environment that is uncontrollable by the defender, such as a battlefield, enabling an adversary to launch physical attacks to capture sensor nodes or deploy counterfeit ones. As a result, an adversary may retrieve private keys used for secure communication and decrypt any communication eavesdropped by the adversary.

1.4.2 Sensor-node resource constraints: battery-powered sensor nodes generally have severe constraints on their ability to store, process and transmit the sensed data. As a result, the computational complexity and resource consumption of public-key ciphers is usually considered unsuitable for WSNs.

1.4.3 *Topological constraints:* The limited communication range of sensor nodes in a WSN requires multiple hops in order to transmit data from the source to the base station. Such a multi-hop scheme demands different nodes to take diverse traffic loads. In particular, a node closer to the base station (i.e., data collecting and processing server) has to relay data from nodes further away from base station in addition to transmitting its own generated data, leading to higher transmission rate. Such an unbalanced network traffic pattern brings significant challenges to the protection of context-oriented privacy information. Particularly, if an adversary has the ability to carry out a global traffic analysis, observing the traffic patterns of different nodes over the whole network, it can easily identify the sink and compromise context privacy, or even manipulate the sink node to impede the proper functioning of the WSN. The unique challenges for privacy preservation in WSNs call for development of effective privacy-preserving techniques. Supporting efficient in-network data aggregation while preserving data privacy has emerged as an important requirement in numerous wireless sensor network applications.

2. REVIEW OF PRIVACY PRESERVATION TECHNIQUES

Many Authors represent many techniques for location privacy, data privacy, network privacy etc.
In [2] Jianbo Yao,Guangjun Wen et.al. have presented DADPP (Data Aggregation Different Privacy-Levels Protection)for data aggregration privacy for wireless sensor networks. Jianbo proposed DADPP used for different levels of data aggregation privacy. At different levels, nodes within the same cluster are divided into many groups and privacy levels are described for each groups that is a node belonging to same group having same privacy level. In[3] Jianbo Yao et.al. represented location privacy of mobile sink node in WSN. Author used the scheme based on local flooding of source and greedy random-walk of sink which means that source does not do have any information about sink and sink uses greedy random walk to collect data from other nodes which prevents predicting their locations and movements from attackers. In[4] Jianbo Yao et.al. presented scheme for source location privacy in WSN. Author proposed a DROW (directed random walk) scheme for privacy of monitoring object when wireless sensor network is used to monitor the sensitive objects. In[5] George, C.M. et.al. proposed a recurrent cluster mechanism for location privacy. Author also described data-oriented and context-oriented privacy preserving techniques. Author used cluster mechanism for preserving privacy of information on location of events or on location of base stations.

In[8] YaHui Li, Ding Yong et. al. have proposed secure message distribution scheme with configurable privacy for a heterogeneous wireless sensor network (HWSN).The characteristic of this scheme is user can only see a message that is intended for him and the sensor node can only generate one signature for all the messages for all the users, which saves the communication and computation cost of the sensor node. In[9] Shaikh, R.A.,Jameel, H. et. al. have presented novel scheme for full network level privacy. For this author used Identity, Route and Location (IRL) privacy algorithm and data privacy mechanism. In[10] Yun Li,Jian Ren et.al. have presented novel scheme for source location privacy. Author represents routing to randomly select intermediate node/nodes before the message is transmitted to the SINK node for maintaining privacy. In[11] Wenbo He,Xue Liu et.al. represented two schemes cluster-based private data aggregation (CPDA) and Slice-Mix-AggRegaTe (SMART) for data aggregration privacy preservation. CDPA includes clustering protocol and algebraic properties of polynomials and SMART includes slicing techniques and associative property of addition.
In[12] Yun Li,Jian RenSensor et.al. have proposed novel schemes for content confidentiality and source-location privacy through routing to a randomly selected intermediate node (RRIN) and a network mixing ring (NMR).RRIN provides local source- location privacy and NMR gives network-level (global) source- location privacy.In[13] Bista, R., Hye-Kyeom Yoo et.al. represent a mechanism for privacy preserving data aggregation. A sink node must be aware of the Ids of all those sensor nodes which aggregate the value of sensors data in order to derive exact result. To solve this problem, set of real numbers is assigned as the IDs of sensor nodes so that a single bit is sufficient to hold ID of a sensor node during transmission of aggregated data to the sink node.
In[6] Sivashankari, S. et.al. have proposed techniques for source location privacy and sink location privacy. Periodic collection and source simulation are the techniques used to provide location privacy to monitored object and sink simulation and backbone flooding are techniques used to provide location privacy to data sinks. In[7] Spachos, P., Liang Song et. al. have presented opportunistic routing schemes for source location privacy in wireless sensor network. In this scheme each node sends a packet to the destination using dynamic path therefore for an adversary to backtrack hop-by-hop to the origin of the sensor data.
In[14] Gurjar, A et.al.proposed a cluster based anonymization scheme for source location privacy.This scheme tells to hide the real node identities during communication,by replacing them with random identities generated by the cluster heads. In[15] Jian Ren et.al. have proposed a scheme to provide both content confidentiality and source-location privacy through routing to a randomly selected intermediate node. In[16] Oualha N.,Olivereau A et.al. have analyzed the existing approaches for privacy protection in WSNs and investigates the approaches that aim at supporting the integration of privacy-preserving WSNs into large scale industrial environments.

In[16] Baokang Zhao et.al. have proposed a new distributed protocol for continuous data collection with privacy preserving in sensor networks called P-preserving.P-preservation means integration of continuous privacy awareness algorithms into existing data collection framework.In[17] Yun Li et.al. have presented a novel based scheme for source location privacy. Mix- Ring based source location privacy can be achieved using three phasing routing i.e. routing to a randomly selected intermediate node, routing in a network mix ring, and message forwarding to the SINK node. In[18] Spachos, P.et.al. have proposed an opportunistic mesh networking scheme for source location privacy. In this scheme, each sensor transmits the packet over a dynamic path to the destination. Every packet from the source can therefore follow a different path toward the destination, making it difficult for an adversary to backtrack hop-by-hop to the origin of the sensor communication.
In[19] Miao Xu et.al. have represented a data dissemination scheme for data privacy and data availability.This scheme leverages the node location diversity presented in typical wireless sensor networks rather than relying on cryptographic techniques.In[20] Kumar, V.et.al. have presented an energy efficient, privacy preserving data aggregation algorithm which also preserves data integrity in WSNs. We analyzed the security of the algorithm and also provided proofs for confidentiality and integrity.In[21] Jhumka, A et.al. provided a novel formalization

of the source location privacy problem, proved the source location privacy problem to be NP-complete, and also provided a heuristic that gives an optimal level of privacy under appropriate parameterization.

In[22] Xinfeng Li et.al. have represented a novel based scheme for protecting the location privacy of base station. This scheme consisting of anonymous topology discovery and intelligent fake packet injection (IFPI).It eliminates the potential threats against base station within topology discovery period.In[23] Rana, S.S. et.al. proposed a novel scheme for source location privacy. A combination of directional antennas, transmit power control and information compression is used to provide lightweight and energy-efficient source location privacy.

In[24] Tscha et.al.have proposed a routing method for source-location privacy in wireless sensor networks of multiple assets. Greedy perimeter stateless routing-based source-location privacy with crew size w, enhances location privacy of the packet-originating node (i.e., active source) in the presence of multiple assets.

3. Discussion and Remarks

Many people work on data privacy, location privacy which includes source location privacy, sink location privacy, Network level privacy. Various techniques have been proposed by many authors that have their own advantages and disadvantages. But as per the survey only few people proposed peer-to-peer network privacy and a lot of research was done on location privacy.

4. Conclusion

This paper represents existing privacy preservation techniques in wireless sensor network. This research mainly concentrates on location privacy, data privacy and network privacy. Each technique has its own pros and cons; this will help us in designing new privacy preserving techniques in wireless sensor network.

References

[1]W. Dargie and C. Poellabauer, “Fundamentals of Wireless Sensor Net- works: Theory and Practice, Wiley, 2010.

[2]Jianbo Yao,Guangjun Wen,” Protecting Classification Privacy Data Aggregation in Wireless Sensor Networks”,in WenWireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on2008.

[3] Jianbo Yao,” Preserving Mobile-Sink-Location Privacy in Wireless Sensor Networks”,in Database Technology and Applications (DBTA), 2010 2nd International Workshop on2010.

[4] Jianbo Yao, Guangjun Wen,” Preserving Source-Location Privacy in Energy-Constrained Wireless Sensor Networks”,in Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on2008.

[5] George C.M,Kumar M.,” Cluster based Location privacy in Wireless Sensor Networks against a universal adversary”,Information Communication and Embedded Systems (ICICES), 2013 International Conference on2013.

[6] Sivashankari S., Raseen M.Mohamed,” A framework of trust management on location privacy and minimising the error rate in wireless sensor networks”,in Optical Imaging Sensor and Security (ICOSS), 2013 International Conference on2013.

[7] Spachos, P., Liang Song, Hatzinakos D.,” Opportunistic routing for enhanced source-location privacy in wireless sensor networks”,in Communications (QBSC), 2010 25th Biennial Symposium on2010.

[8] YaHui Li,Ding Yong,Jian feng Ma,” Secure Message Distribution Scheme with Configurable Privacy for Heterogeneous Wireless Sensor Networks”,in Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on22008.

[9] Shaikh R.A., Jameel H., d'Auriol B.J., Sungyoung Lee, Young-Jae Song, Heejo Lee ,” Network Level Privacy for Wireless Sensor Networks”,in Information Assurance and Security, 2008. ISIAS '08. Fourth International Conference on2008.

[10] Yun Li, Jian Ren,” Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks“,in INFOCOM, 2010 Proceedings IEEE 2010.

[11] Wenbo He, Xue Liu, Hoang Nguyen, Nahrstedt K., Abdelzaher T.,” PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks”,in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE2007.

[12] Yun Li, Jian RenSensor,” Preserving Source-Location Privacy in Wireless Sensor Networks”,in Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on2009.

[13] Bista, R., Hye-Kyeom Yoo, Jae-Woo Chang," Achieving Scalable Privacy Preserving Data Aggregation for Wireless Sensor Networks ", in Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on2010.

[24] Gurjar A., Patil A.R. B.," Cluster Based Anonymization for Source Location Privacy in Wireless Sensor Network", in Communication Systems and Network Technologies (CSNT), 2013 International Conference on2013.

[15] Jian Ren, Yun Li, Tongtong Li," Routing-Based Source-Location Privacy in Wireless Sensor Networks",in Communications, 2009. ICC '09. IEEE International Conference on2009.

[16] Oualha N., Olivereau A.," Sensor and Data Privacy in Industrial Wireless Sensor Networks", in Network and Information Systems Security (SAR-SSI), 2011 Conference on2011

[17] Yun Li., Jian Ren.," Mixing Ring-Based Source-Location Privacy in Wireless Sensor Networks", in RenComputer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on2009

[18] Spachos P., Liang Song, Bui F.M.," Improving source-location privacy through opportunistic routing in wireless sensor networks", in Computers and Communications (ISCC), 2011 IEEE Symposium on2011

[19] Miao Xu, Wenyuan Xu, O'Kane J.," Content-Aware Data Dissemination for Enhancing Privacy and Availability in Wireless Sensor Networks", in Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on2011

[20] Kumar V., Madria S." PIP: Privacy and Integrity Preserving Data Aggregation in Wireless Sensor Networks", in Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on2013

[21] Jhumka, A., Bradbury, M., Leeke M.," Towards Understanding Source Location Privacy in Wireless Sensor Networks through Fake Sources", in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on2012

[22] Xinfeng Li, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, Ming Gu," Enhanced Location Privacy Protection of Base Station in Wireless Sensor Networks", in GuMobile Ad-hoc and Sensor Networks, 2009. MSN '09. 5th International Conference on2009

[23] Rana S.S., Vaidya N.H.," A new 'Direction' for source location privacy in wireless sensor", in Global Communications Conference (GLOBECOM), 2012 IEEE2012

[24]Tscha, Yeonghwan,"Routing for enhancing source-location privacy in wireless sensor networks of multiple assets", in YeonghwanCommunications and Networks, Journal of112009

[25] Kiran Maraiya, Kamal Kant, Nitin Gupta," Application based Study on Wireless Sensor Network", in International Journal of Computer Applications (0975 – 8887)Volume 21– No.8, May 2011

[26]A dissertation thesis proposal on"Privacy preserving protocols for wireless sensor networks", by Jiri Kur.

[27] Prakhar Gupta, Meenu Chawla ,"Privacy preservation for WSN: A Survey", in International Journal of Computer Applications (0975 – 888) Volume 48– No.3, June 2012

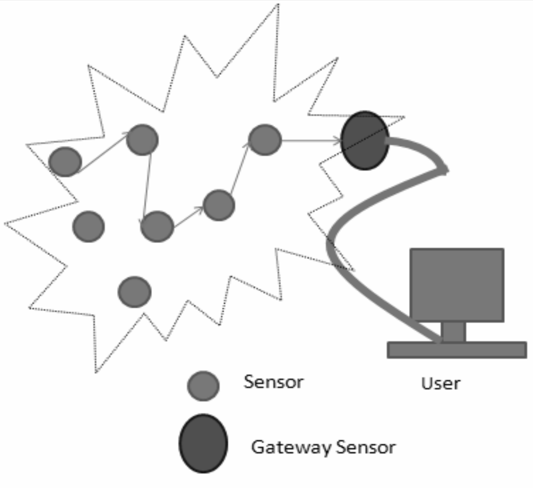

Fig.1.Architecture of wireless sensor network

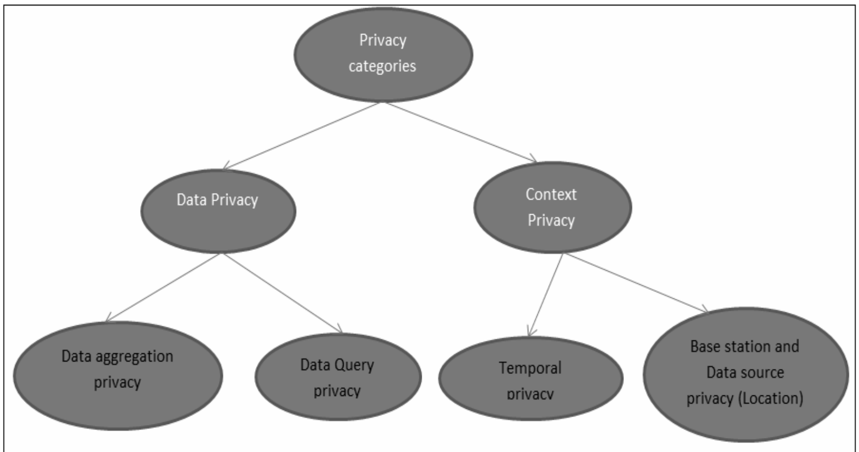

Fig.2.Wireless sensor network privacy