Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Privacy Preservation Schemes in Wireless Network

Mayur R. Tawalare
Project Scholar, Dept. of Computer Science and Engg.,
G. H. Raisoni College of Engg., Nagpur,
(MS), India

Sonali Nimbhorkar
Asst. Professor, Dept. of Computer Science and Engg.,
G. H. Raisoni College of Engg., Nagpur,
(MS), India

Abstract: ***Wireless sensor network is used widely and it is a key technique in the application of military which are used in daily life. There is an some fundamental architectures that one from compromising a sensor and server and another is to compromising a sensor, server and a storage capacity nodes between the two tier architecture we have to evaluated the second type that have number of advantages in various terms that is energy usage, data transmission and the last one is data computation. As the time two tier wireless sensor network have some advantages related to the security that is the major concern in the two tier architecture. The three main problems is the first, sensor that can located in unfavorable areas can be unauthorized will be replaced the third party that can send the fake data. Secondly, the malicious attacker could be installing new sensor node with a valid secret keys that send a fake data to the receiver node and distract the server. Third is to the receiver node that could be negotiating and expose data received from the sensor. So that's why the server must validate the sensors before acquire the data from them, recognize whether a key was deflect and determine the key which one and to handle the nearly all general queries while to preserve the data privacy received from the data storage node. We have to construct a novel solution that would be using a Non- Adaptive Group Testing that allow a sensor to execute that different task successfully and professionally. The overall conclusion is to protect with a very high probability in contrast to attack that get guess sensor data and to secure the data privacy.***

Keywords:- Wireless Sensor Network, Authentication, Privacy-preserving, Group Testing.

I. INTRODUCTION

In an implementation and the research areas one of the largest skyrocketing sector in WSNs. Observe that this technology that would be change the world ever since 2003[1]. In the reference [2] we observe that the various applications of WSNs divided into three types. Those are monitoring the space, monitoring the relations of the things and monitoring things with each other and surrounding space. The importance of WSNs is they have to capability to survive a ruthless environment condition and manages the node collapse, scalability, abandoned operation and a huge range of formation. WSNs are a multi-hop network that has to combine a multitude of small independent devices. Sensor is not only the receive message or any command or instruction from their nearby resident but also send the information. The resources of WSNs are restricted they have finite computation strength, very slow, processing speed, minimum memory space and restricted power resources. In the previous year's researchers can done more efforts to solve that problem to upgrade the performance of WSNs system.

By improving the popularity of WSNs system and the people responsiveness of the self defense, the problem is data privacy in WSNs is established to develop. Those days more and more WSNs are executed in ordinary areas where high confidentiality is requires. Confidentiality of location is essentially concern the location of sensors or to the base station and primary condition timing mainly pointed on the time when the data is to be produced at the data sources. This type of privacy is necessary for mobile devices. For example:- suppose any opponent that will known about the location of the people at everyday, so he can easily gather the people behavior and this is risk about the people security. In WSN the preservation of information is an important aspect for service users. It is most challenging fact to design a protocol for data aggregation and privacy preservation. It is difficult to design technique for privacy preservation of location based service. Research work focus on privacy preservation technique in mobile for international domain. The mobile devices are different from each other. It is complicated to map the preserving technique. A various mobile device stand with respect to its location services that contain routing map, service plan and game. There is a improvement in the location based service that can be organize in the privacy of location confidentiality and information is available by means of sharing of information [1].

In the following figure the problems of related to the data privacy is WSNs can be classified.

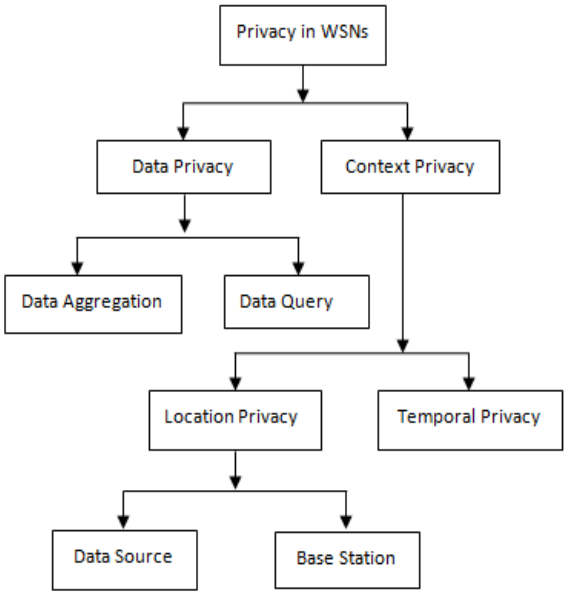

Fig 1:- Taxonomy of privacy-preserving for Wireless Sensor Network

From the above figure we have to recognize one phase of the privacy in WSNs research is data aggregation. This is mainly fuscous on the privacy preservation on data aggregation. Number of methods can be developed to protect the data privacy in WSNs data aggregation that is CDPA, SMART, and DADPP. In that paper we have to plan a new method which is to be encouraged by the context data privacy data aggregation (CDPA). In my scheme has lower computational cost or overhead than CDPA and it is more secure. If some packet is not loss this scheme is very useful or efficient without publish any private information [2].

II. SYSTEM ARCHITECTURE AND DESIGN GOALS

This section can describes the system architecture and major design goals of the paper

A. System Architecture:-

In Wireless Sensor Network (WSNs) architecture that taken into consideration consists of key authority agreement, data store units and the deployment of sensors node around the surface.

Key Authority: - Key authority agreement is a secure which generates a key and sends to the owner's mail in order to provide security to that key. Each sensor node firstly to the data owner registration phase that that the data can be maintain by creating groups and each sensor has its own respective group ID which can be used to login an another server. There is no need to be always online for the authority key.

Data Store Units: - It is secure which can be used to store data according to its respective ID's of group. Data stores unit can store data which is generated by the sensor nodes and gateway can be used to secure the connection between service nodes and source nodes. Data store unit has power to support the adjure frequency bandwidth in order to transfer to the different service provider.

Generally the data is generated by the sensor node and sensor node can transmit the data to their respective mediator node for this routing protocol can be build.

Sensor Node:- In the paper study the sensor node can collect atmospheric data and perform a communication between each other for transformation of sensor data to the data store unit. The wireless medium can be used to send the data from sensor node to the data store unit.

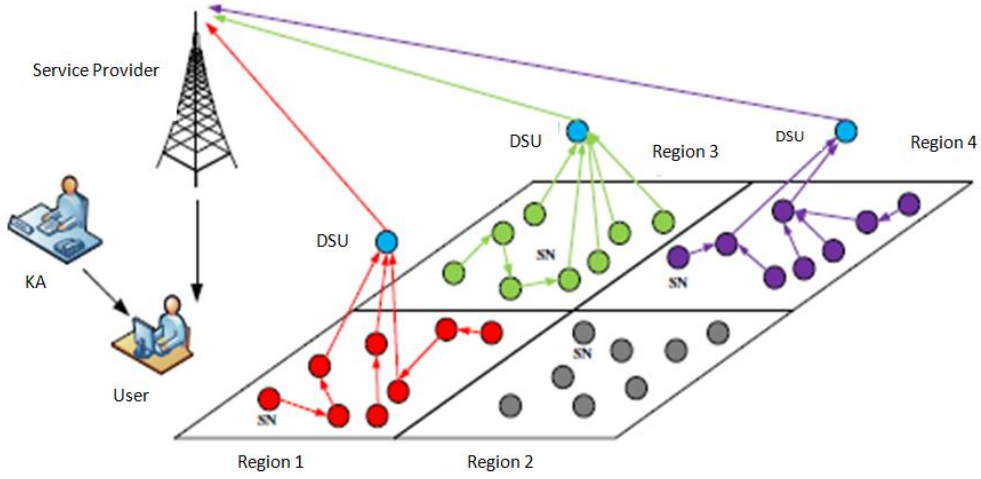

Fig 2:- System Architecture

B. Design Goals:-

In order to achieve security of data of wireless sensor network we required to gain some security goals

Confidential Information:- Confidentiality of information is the major concern in the WSN's. Sensitivity of the information or message can be protected for the malicious third party attacks. It is important to provide confidentiality to the wireless sensor network.

Substantiation:- It is nothing but the authentication of the user authenticated user can only access the data privacy schemes can provide authentication in order to differentiate real users from unauthorized users. It also provide authentication to the service provider.

Data Privacy:- Aim of the data privacy is used to protect data users from intruder attacker node. Not from malicious node but also from service provider source. Privacy preservation scheme can be develop in order to prevent data from the unauthorized server of the network. Data privacy can be maintained by using data aggregation and data query scheme of the data privacy preservation.

Basic designs goals to developed method in which authentication of user can be provide. The authentication is done by implementing server name as authentication server. Three-tier architecture can be build to filter the data from different domains key agreement protocol can be implemented by the security of the key. Grouping can be done for better performance of the server. Queries can be executed in order to encrypt the data.

III. SYSTEM MODEL

A. Network model and presupposition:-

Implementation of roaming protocol consist of multiple server these server are home server, foreign server and authentication server. Three-tier security can be constructed in categorize to implement a network mode contain three domain.

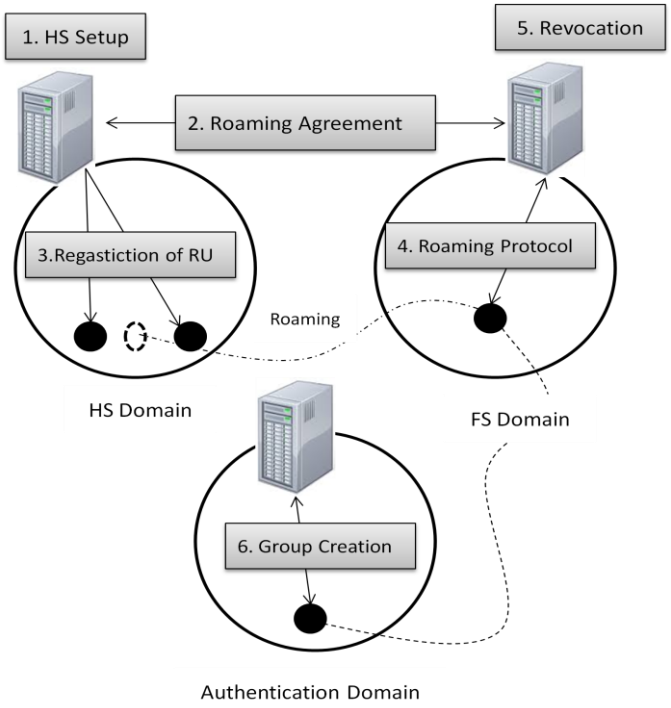

Fig 3:- Network model of the proposed System

In the network model of the proposed system firstly user can register in the home server. Each user has its own user ID and password. Foreign server and authentication server are play the role of private key generator that key directly send to the data owner mail ID with total security. Foreign server can create a group of user and from grouping duster each group members have unique group ID by using that group ID, user can login into the authentication server. Overall data filterization can be done in the authentication server.

B. Trust Presupposition and attacker Model :-

Implementation of server contains some assumption for the betterment of the roaming protocol. Generally it's assumed that home server is the reliable entity because it can collect the information of registered user ones user entered in the foreign server. Home server can trace the location of registered user and home server also identity that register user are authorized or not. The secure channel can be implemented using three-tier architecture. The server can also control the communication channel and protect the information from modifying it or injecting some virus in the file by third party attacker or third party malicious node. The objective of attacker model is to inject unsigned authentication of a roaming protocol by negotiating requirement of the foreign server. In foreign server may be there is a malicious attack it attempts to gain the information of data owner. Therefore authentication servers can be implemented to provide complete security.

IV. SECURE KEY DISTRIBUTION

The key can be generated by authentication secure. It is a random key generator called as pre distribution of random key. Algorithm can be implemented in which digits, alphabets are declared randomly by using combination of keywords key can generated. In the privacy preservation scheme can implemented k number of keys that can be stored in privacy source node in the network. Keys can be shared between sources to the source for the secure communication. The key also kept for the source to source communication. There are two key exchange schemes are implemented.

1. Server to Source Key Exchange.
2. Source to Source Key Exchange.

A. Key Establishment between Server to Source:-

The network contains number of source nodes and server. The random number of key can be shared between these server and source node. Basically the channel or communication medium as not much secure to share secret keys between source and server. Each source node has some shared keys. Attacker can easily inject any malicious data and easily launch any attack in order to decrypt the communication of source nodes in the network. For avoiding the attack mounted by the third party attacker the pre distribution phase can be implemented. The authentication server can create random key and key establishment can be done between sources to secure pair. The shared key can be distributed according to the respective group ID. That group ID can be private in order to preserve data in the network. The key can be randomly attierd and recorded for each server to source pair. The order of the key can be stored in the secure storage unit of respective source. If suppose a new data owner can login likewise group ID can be created and key can be randomly reloaded and store that key into the server side randomly the storage can be offline.

Each Source node can communicate with the server through key agreement. To achieve secure communication first data owner can login into the home server likewise in the foreign server can create the groups for the data owner member, each member can have some unique identity to login the authentication server. For the generation of the key/ private key random numbers can be declared and key directly send to the data owner login mail ID. It is totally secure communication medium in which each server can have its own security mechanism each key is different source node for securely source node. The database also mechanism in the server only authentication user can get the shared private key. Because at the time of data owners login into the network home server can already check the real identity of data owner whether it is a real user or authorized user or not. If there is any malicious client want to enter into the network then home server cannot allow that malicious client to interfere in the network.

B. Source To Source Key Establishment:-

We also implemented source to source key agreement. We assume that key establishment between server to source is highly secure. Therefore key establishment can be done by server, it cannot be perform directly between source to source node. In the observation it is clarify that some keys are same for multiple source node. Therefore the next task is to implement key for each source to source communication and at every key generation each key is different from other key. It may be observe that in that network in the source have same key that it becomes very easy to decipher the message of other node in the network. If the communication can be perform in between source node1 and then the source node 2 and after that source node 3 can accomplish the information or message that move between the source of node 1 and then the source of node 2. To avoid this type of situation algorithm can be implementing.

In that the routing protocols for source to the source key establishment, each of the source node can permute/ adjust the keywords in the server of the random key that are detected for that the source to the source node can separately passes the permutation functions of the server. If the successful message comes from the server about key then one of the server node can send other random number in order to generate key in the network for safe communication.

V. SECURITY AND PRIVACY DETERMINATION

Security and privacy determination can be purposed against the attacks. Protocol contains some counter measures implemented in the privacy preservation scheme these counter measures are as follows.

A. Identity Maintenance :-

Most of the user done it show real identity if they entered in the roaming reason. They wish to remain unknown at the time they enter in the wireless network for privacy reason. At the time when data owner can login or register into the home server the private group ID can be created by each group member. It is nothing but the cluster formation can be done in the wireless sensor network. By using this unique group ID data owners' data owner can login into authority. Only this identity can be used for the communication. There is no need to display the real name at the time of the communication. But it real identity can be store in each server while the communication is going on. The data owner descriptive identification can be known to the trusted authority only and it can be tracked by the unique group ID assigned to each user.

B. Access Control :-

The implementation of work only allowed to the legitimated user can gain access control while user can enter into the network. In order to access the network the respective user can successfully register in the network cluster along with the security keys. The attacker can easily get that valid private security key or signature of trusted authority and it is not authenticated by the wireless network. Network can be implemented in away such that any attacker cannot enter in the network also attacker not try to access the data in the communication medium.

VI. IMPLEMENTATION PLAN

The implementation plan consists with the registration phase in the home server. Data owner can login into the home server. After competition of registration phase foreign server can collect the information of owner from the home server. The work of the foreign server can start, foreign server creates group for each data owner. Each data owner have unique group ID. By using this unique ID data owner can join ring group of foreign server.

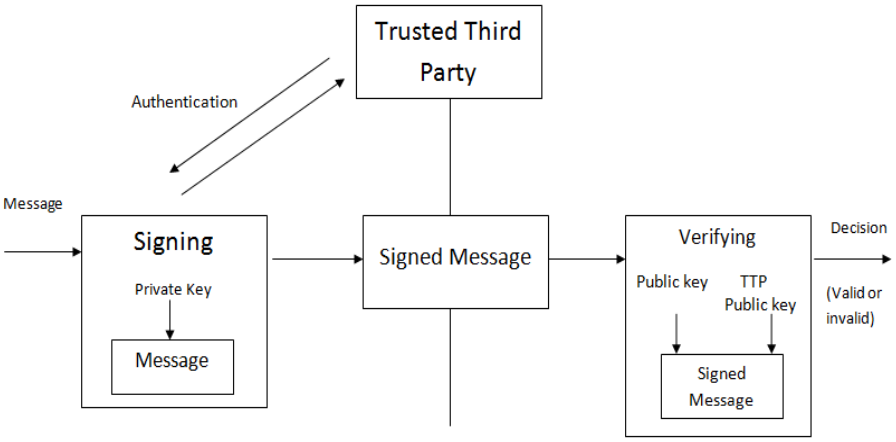

Fig 4:- Flow of methodology to be employed

After the creation of groups the information can be stored in the data store unit of authentication phase. Authentication phase can be create key by using the combination of number of alphabets the key can be generated. For security purpose that key directly send to the mail ID of data owner. Verification process can be done on that private key then data can be upload in the network and it is accepted by foreign server.

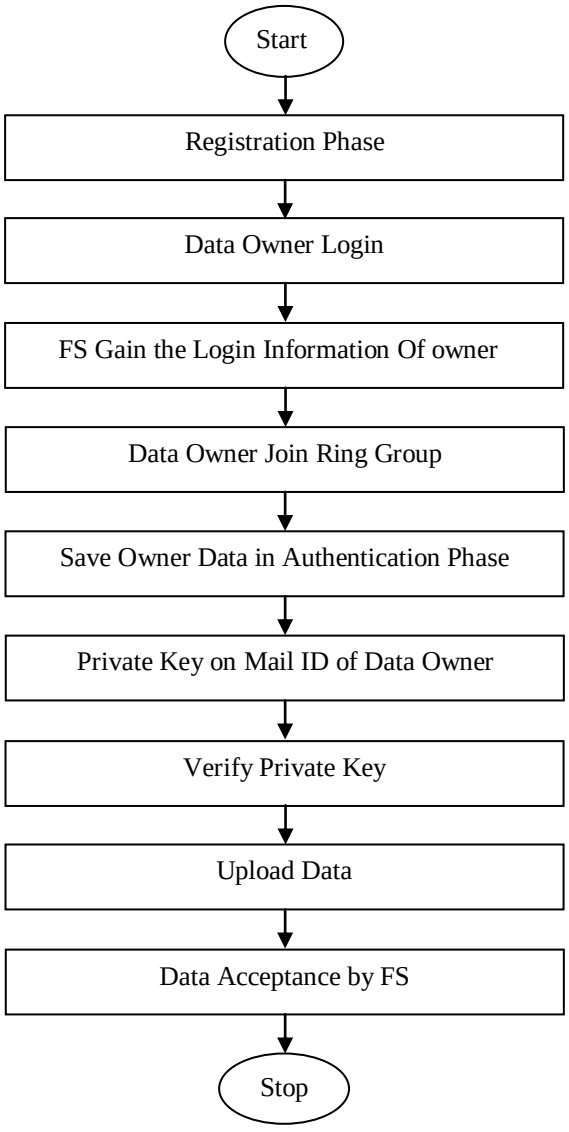

Fig 5:- Work Flow

VII. RESULT AND ANALYSIS

Roaming services in the wireless sensor network provide people more flexibility and better for communication. The existing privacy preservation techniques in wireless sensor network mainly focuses 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. The proposed system will provide a novel protocol to achieve privacy-preserving universal authentication for wireless communications. It is able to provide privacy about mutual authentication with user anonymity and is effective in protecting from various attacks. The work is basically focuses to protect the location privacy of users, preserve the privacy of roaming users by using linking information and to defend the Identity of user by using group ID and Group Name. We evaluated the efficiency of our protocol by comparing it with existing protocols and by implementing a prototype of our protocol.

Table No. 1:- Comparison of Functionalities and Performances of Roaming Protocols

Roaming protocol	HS	Anonymity	Security of Session Key
G.Y.10 Protocol 1[5]	Offline	Weak	0
G.Y.10 Protocol 2 [5]	Online	Strong	0
G.Y. 08 [9]	Online	Strong	0
D.H.11 [16]	Offline	Strong	0
D.H.12 [18]	Offline	Strong	X
C.C. 10 [20]	Online	Strong	0
Our Suggested Protocol	Offline	Strong	0

0: Secure X: Not Secure

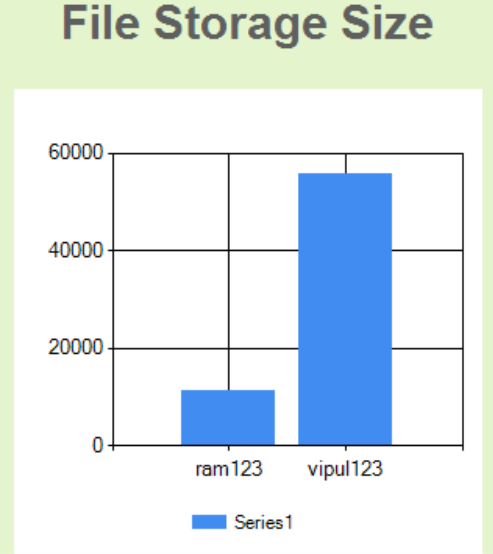

Fig 6:- Comparative analysis of File Storage size of users

REFERENCE

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," ComputerCommun., 2010, doi: 10.1016.

[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans.WirelessCommun., vol. 9, no. 1, pp. 168-174, 2010.

[3] D. He and S. Chan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Commun., 2010, doi: 10.1007/s11277-010-0033-5.

[4] C.Y. Chow, M.F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks", IEEE Trans. Mob. Comput., vol. 10, no. 1, pp. 94-107, 2011.

[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 on 2013.

[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 on 2013.

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

[8] H. Mun, K. Han, Y.S. Lee, C.Y. Yeun, and H.H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks", Math. Comput. Model., vol. 55, no. 1-2, pp. 214-222, 2012.

[9] Yun Li, Jian Ren," Source-Location Privacy through Dynamic Routing in Wireless Sen-sor Networks",in INFOCOM, 2010 Proceedings IEEE 2010.

[10] 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.

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

[12] 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.

[13] 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 on 2013.

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

[15] Oualha N., Olivereau A.," Sensor and Data Privacy in Industrial Wireless Sensor Net-works", in Network and Information Systems Security (SAR-SSI), 2011 Conference on 2011.

