ISSN: 0369-8963

Performance Analysis of various Schemes for Source-Location Privacy Preserving Wireless Sensor Networks

R.PITCHANDI@SANKARALINGAM[1], DR. C. ARUNACHALAPERUMAL[2], DR .E.A. MARY ANITA[3]

[1]Associate Professor, MCA Department, Madha Engineering College, Chennai-600 069
[2]Professor, Department of ECE, S.A. Engineering College, Chennai-600 077
[3]Professor, Department of CSE, CHRIST University, Bengaluru -560 074

Abstract

Wireless Sensor Network (WSN) is a recognized environment used in many applications that require monitoring events. They lack in maintaining confined boundary and so they are prone to unauthorized interception and detection. Privacy has become an essential issue in finding a solution for deploying the environment of WSN. In specific this paper deals with the study of solutions related to Privacy that preserves the source location on WSN. Various methods ensure confidentiality of the messages by encrypting the contents. Adequate addressing on source location privacy is bit complex due to intensive computations on cryptographic algorithms that are not adaptable for WSN. Conventional methods related to authentication and encryption fail to preserve privacy on managing sinks location. To complicate the process every node generates fake messages depending on their corresponding nodes. But these fake messages consume more energy from the nodes that impacts the lifetime of the network. This paper provides us the overview on the source location privacy along with the essential concepts related to it. The concepts are summarized and solutions are categorized based on their techniques. The limitations of the various methodologies are found and solutions are classified accordingly.

Keywords: *WSN privacy, Source Location Privacy (SLP), Aggregation of data, Sinks location and Aggregation of privacy*

Introduction

Wireless sensor networks depend on wireless communication that serves as a media for broadcasting and prone to many security threats. They use expensive transceivers for initiating and developing interactions among the networks and they detect the flow of message and are traced back to where the source message was initiated by moving through reversed path [1][2]. The objects or living organisms can be protected and their information related to location must be hidden. The ultimate aim of privacy preservation on source location is to conceal the source location of the message and it becomes complicated while tracing the message back to the source [3],[4]. In phantom routing the source node does not send the data directly to the sink, here the source transfers the data

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

to the node belonging to the phantom that depends on the shortest path of the sink. The existing routing schemes are based on the phantoms which consists of the nodes directly routed to the sink and their trace back fail to find the target. Direct solution is to have various routes to the sink. It is complex for the attackers for determining the route where the data resides. Hence source location privacy is improved. Energy consumption is the major drawback in this method. WSN is comprised of small nodes that are deployed in geographical area. The network senses the environment and reports wherever necessary. They lack in resistant packaging and insecure channels where the network is exposed to various attacks from environment. WSN is designed to support the sensing devices and their process of communication by data transfer that are collected by sensors and directed to corresponding sinks. This nature of broadcasting causes many attacks and affects the performance. Recent studies suggest new technologies for protecting the anonymity of the source and destination node. It is observed that minimal focus is given for obscuring the geographical location of the sink node. Sink nodes plays a key role in the network, if they are disabled by the attackers, transfer of information from monitoring area to the centre is affected. The algorithms proposed for transmitting the data senses the data via small set of paths that are fixed. Through this pattern in traffic are easily identified that reveals the sink node. From the point where flow converges, location of the sink is identified by traces of the traffic. Another clue for the adversary is the nodes that are present near the sink forwards a greater number of packets compared to the nodes that are located far away. This feature becomes the central point of failure where the entire sensor network is disabled and sink node is destroyed. Therefore, contributions related to privacy of sink is very limited in the literature, hence this paper summarizes entire solutions provided in the existing literature and give direction for future work.

Background

The nodes in WSN are deployed and organized based on the environment for which it is developed. They contribute various phenomenon while inspecting the network area. While considering tracking and monitoring applications the following architecture was adapted: an area is monitored by the nodes and identify a subject. A subject differs based on different application; it can be a human, vehicle or animal. Once the node identifies a subject it creates few *sinks* [5][6]. A *sink* is defined as a node with high capacity for storage, power of computation and an effective power supply compared to other nodes. Main function of the sink is to collect all data and send it to the server or it permits

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

extraction of data manually. The process of node sensing the subject is termed as an event [7].

Best example to explain source location privacy is panda hunter game [8]-[12]. The duty of the nodes is to track the location of a panda within a particular area. Once the panda is sensed it informs the sink by sending a message that travels through nodes in the intermediate to the sink. If the hunter is out to hunt a panda he might trace the information through WSN to kill the panda. Hence the panda has to be protected from the adversary by hiding the location of the source through *source location privacy* (SLP). It must ensure confidentiality between two nodes. The flow of message should be in such a way that it does not reveal the source node location. Content privacy has to be maintained among the messages interchanged between wireless networks. It hides the node location, flow of traffic and identity of the nodes [9]. For providing source location privacy we have to analyse the counter traffic which is considered as an unsolvable issue compared to SLP in WSN. The suggested best solution is anonymity based and routes that are untraceable which was indicated by Chaum [13]. The solution was based on mixing messages and digital pseudonyms termed as MIX-net.

Solution based on categories

This section defines the set of categories based on the view of adversaries about the network. The categories are as follows: random walk, delay, geographic routing, use of fake data sources, anonymization of location, routing of cross-layer, network code, limitation in node detectability.

(i) Random walk:

This approach encourages the packets to take up a route that is chosen to be random in the network. This walk appears completely random through the network by which the traffic analysis of attackers is predicted. Ozturk and team [14] proposed a solution through rumor routing of randomly selected intermediate node from Li et al [15][16]. The suggested solution mechanism are selection of nodes through multiple intermediates that are angle based [16], random walk that is directed [17], support scheme for location privacy [18], opportunistic routing [19], phantom single-path routing with locational angle [20,21], random routing schemes [22,23].

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

(ii) Geographic Routing:

Solutions related to geographic routing make use of the nodes physical location in addition to the geographic routing algorithms for routing the packets in WSN [24]. The algorithm picks up the position of the nodes, their neighbours, and sink for routing the

packet from source to the sink node. The solution is based on the additional methods which include synonyms, encryption and random intermediate selection of nodes for hiding the flow of traffic from the attackers. The solution under this category is sink toroidal region routing [25], route and location privacy, reliable identity.

(iii)Delay:

The solution for this category alters the flow of traffic by buffering the packets that are incoming and holds a packet for a particular period of time and forwarding it when required. As a result of which the order of nodes is altered and packets are sent in random order. This affects the pattern of the traffic that tends the adversary hard to predict the actual source. The solutions identified are probabilistic reshaping and its extended version [26] and rate controlled adaptive delay [27].

(iv)Using fake data sources:

Fake traffic is introduced to compensate with real traffic in such a way that attacker is not able to identify whether it's a real traffic or fake traffic. Proposed solutions are cloud-based scheme for protecting SLP [28], dynamic bidirectional tree [29], fitted probabilistic rate [30], globally optimal algorithm [31] and many similar mechanisms.

(v) Anonymization of network location:

Here either the node identity or node location is concealed. Solutions on this categories are anonymous communication scheme[32], anonymous path routing [33], cryptography based anonymity scheme [34], anonymous routing protocol that are destination controlled by sensornets [35] and reverse hashing ID randomization [36].

(vi)Routing cross-layer:

Here beacon frames are used that are mainly used for network maintenance for sharing information on events that are sensed. Adversaries focus only on packets at network level and fail to check on the exchange of information and skip finding the real source. The two suggested solutions are cross layer solution and double cross layer solution [37].

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

(vii) Network coding :

Here the message is split up by the nodes into smaller parts and transmitted. They are forwarded through different routes to the sink.

(viii) Limiting node detectability:

Solutions are limited to transmission power of nodes that make the adversary hard to detect. Proposed solutions are silencing through anti-localisation [38], context aware location privacy [39], hidden anchor [40], minimal radio transmission power[41] and multi co-operator power control [42].

Existing methodologies on Source location Privacy

The existing methodologies consist of routing protocols for protecting the SLP and maximize the lifetime of WSN. This section summarizes the methods in detail.

(a) A diversionary routing scheme that is tree based for preserving SLP

Hide and seek strategy is used for creating diversionary routes and their path that directs to the sink from the source. Here it is observed that each diversionary route emits events that are fake. The network lifetime is maximized and depends on the nodes with high energy consumption and minimizes it in hotspot generated environment. Privacy is preserved and network lifetime is also maximized. Here they have identified a direction-oriented attack against phantom routing. Comprehensive analysis is done that defeats direction- oriented attack. Theoretical and experimental results prove that the scheme is effective on SLP and network lifetime maximization [43].

(b) Sink Location Privacy Protection protocol(SLPP)

Bidi Yang and team proposed a protocol SLPP [44], which was easy to implement without affecting the lifetime of WSN. For confusing an attacker fake message is generated by every node that takes part in the network. The messages are dependent on number of the nodes children. The simulated results prove that this protocol hides the location of the sink effectively. This type of transmission consumes additional energy yet the lifetime of the network is not affected.

(c) Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks

Message authentication is a productive way to thwart corrupted traffic and unauthorized messages from getting transferred in WSN. For providing this effort polynomial-based scheme was introduced. Drawback arises when degree of the

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

polynomial is difficult to be identified after it reaches the threshold level. When threshold is minimal compared to the messages being transmitted in the network the attacker can easily recover the polynomial. Hence a scalable authentication scheme based on elliptic curve cryptography (ECC) is introduced [45]. When intermediated node authentication is enabled the scheme allows the node to transmit numerous numbers of messages. It also provides message source privacy. The analysis, based on simulation proves that message source privacy is maintained in terms of computational overhead.

(d) Quantitative Measurement and Design of Source-Location Privacy Schemes

Computationally intensive cryptographic algorithms fail to ensure content encryption. Quantitative measure of SLP is proposed and analysed in this work. Through this measure vulnerabilities are identified of various SLP schemes in WSN. Proposed scheme provide SLP through routing for randomly selected intermediate node (RSIN) and network mixing ring (NMR) [46]. The scheme has achieved high delivery ratio and efficient results are obtained.

(e) The Three-Tier Security Scheme with mobile sinks

Mobile sink is essential in WSN for efficient accumulation of data, localized sensor reprogramming and revoking and distinguishing compromised sensors. Existing predistribution key schemes give way to new security challenge because an attacker can easily obtain large amount of information. Hence three tier general framework security scheme was developed by Amar asheed [47]. Basic component here is pairwise key pre distribution and the framework comprises of two key pools for mobile sink for accessing the network and another one is pairwise key establishment between the sensors. Authentication mechanisms are strengthened by reducing the damage caused by replication attacks. This scheme has proved greater network resilience for mobile sink replication attack when compared to polynomial pool-based scheme.

(f) Enhanced scheme of Communication Protocol for Anonymity and Location Privacy in WSN

Communication protocol is developed for maintaining anonymity and privacy of location in WSN by Abdel and team [48]. It is measured by anonymity, observability and safety period. A network model is presented that protects the network against active and passive attacks using different adversaries that is local, semi-global and global. The

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

anonymous model consists of three different phases deployment, icebreaker and communication phase.

(g) Maintaining Location Privacy in Multiple Sink Using Zone Partitioning Approach in WSN

The adversary focuses on the sink node defined as data aggregation point for WSN. Hence sink location has to be protected from the attacker. This work proposed modifies the existing sink location from the adversary by partitioning the nodes in the network that contains multiple sinks into different zones where the packets are forwarded to respective zones where the sink belongs. The intermediate nodes generates irrelevant fake packets and forwards it to sink. Performance analysis is performed on computing time, throughput, packet delivery ratio, end to end delay and consumption of energy. The scheme also protects the network from heavy traffic [49].

(h) Privacy-Preserving Access Control scheme with Distributed access for Single-owner Multi-user Sensor Network

This novel approach ensures preserving privacy over distributed access control called Pricess [50], which is single owner multi-user sensor network. Users holding same access privileges are grouped into same cluster by the network owner. The user signs a query command and transmits to the sensor nodes. The nodes will respond only after signature is validated of the query command. The signers identified by the verifiers without revealing the member, hence privacy is preserved and access control is achieved. The proposed protocol is implemented in IMote 2 motes. The results generated shows the efficiency of Pricess and this is the first ever access control technique implemented in WSN platform.

(i) WSN against Adversarial Localization

This paper studies the issue related to defending factor against localization of adversary in WSN [51]. The attempts made by the adversary to reveal the physical location of the sensors in the network. This is accomplished by the network by moving in the network while eavesdropping for communication messages that are transmitted by the sensors. The physical properties that are measured are Arrival angle, Strength of the detected signal. The sensor network defends adversarial localization and the challenge that arises is to hide from the adversary and localize them. Here only important sensors

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

communicate through messages. The performance is evaluated by extensive simulations and found to be effective.

(j) Opportunistic Routing for Enhanced SLP

SLP faces challenges threatening the deployment of sensor networks when sensitive objects are monitored [52]. For enhancing the SLP an opportunistic routing schemes was proposed. Here each sensor transmits the packets in dynamic path to destination. In this type of routing each packet from source may follow different path to destination that makes adversary to backtrack step by step to origin. This is suitably demonstrated with efficiency in practical applications.

(k) Routing based SLP in WSN

The privacy service is complicated since the sensor nodes are of minimal cost and minimal power radio devices. The computation on cryptographic based algorithms becomes intensive along with their broadcasting protocols for WSN. The scheme proposed is randomly selected intermediate node (RRIN) [53]. The protocol choses an intermediate node in the sensor domain while transmitting the data packet by randomly selected nodes to the destination. The source node does not have accurate information about the sensor nodes. The location that is relative guarantees that message packet has forwarded to environment of intermediate node. The node that is present in the last of routing path must be able to deliver whether randomly selected node exist or not. The node in the intermediate node routes the message to destination node.

Methodologies of location anonymity in Wireless Sensor network

Proposed Solution	**Attacks**	**Network view**	**Information Exposed**
ACS[70]	Locating a node, identity analysis attack	Local	Exposed protocol not mentioned
APR[71]	Eavesdropping and tracing hop-by-hop	Local	Topology exposed
DCARPS[72]	Eavesdropping and tracing hop-by-hop	Global	Topology exposed

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

EAC[73]	Traffic analysis and locating a node	Global	Topology exposed
Probabilistic DCARPS[72]	Eavesdropping	Global	Topology exposed
HIR and RHIR[73]	Compromising nodes	Global	Exposed protocol not mentioned
MQA[74]	Eavesdropping and tracing hop-by-hop	Global	Aggregation protocol
PhId[75]	Traffic analysis	Local	Topology exposed
SAS&CAS[76,77]	Compromising node and limited traffic analysis	Global	Topology exposed

Table 1 : Summarized view of location anonymity solutions along with the possibility of attacks

Summary of the Results

Scheme	**SLP Protection**	**Energy Consumption**	**Network Lifetime**	**Delivery Reliability**
TDR	Significantly higher than RIN in near network border regions due to distribution of large amount of fake packet traffic in diversionary routes.	Significantly higher than RIN due to distribution of large amount of fake packet traffic in diversionary routes.	Comparable with RIN due to minimized energy consumption in the near-sink regions.	Significantly lower than RIN due to packet collision events.
DDR	Significantly higher than RIN due to flooding of fake and real packets inside the blast ring.	Significantly higher than RIN due to packet flooding inside the	Significantly shorter than RIN due to flooding of fake and real packets inside the blast ring.	Lower than RIN due to packet collision events when source node is outside of the blast ring.

https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

		blast ring.		
FPR	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Shorter than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly lower than RIN due to packet collision events.
PRR	Slightly higher than RIN due to distribution of small amount of fake packet traffic.	Slightly higher than RIN due to distributio n of fake packet traffic in the near-sink regions.	Shorter than RIN due to distribution of fake packet traffic in the near-sink regions.	Slightly lower than RIN due to packet collision events.
RIN	Low	Low	Long	High

Existing Data Aggregation schemes on SLP

Private data aggregation has a great challenge in performing efficient aggregation at intermediate node which protects the sensitive data privacy. Data aggregation protocol consists of two categories: (i) Encrypted based protocol and (ii) Unencrypted protocols. Privacy preserving techniques is further classified into hop-by-hop encryption, computation in Multi- party and privacy homomorphism.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

Hop-by-hop cryptography scheme ensures privacy in communication with the presence of third party. Here encryption and decryption are performed for every hop. The aggregator decrypts each received message into plain text and then that is aggregated to a function that encrypts the aggregated result before being forwarded. Once compromised, node of adversary can easily hold of the sensitive data. Here end-to-end data concealment is maintained for protecting privacy [54-58].

Secure multi-party computation scheme is a part of technique based on cryptography which was proposed by Yao [59]. The aim is to generate methods which enable the parties for creating a function through inputs. Privacy preserving is applied to data mining, database query and intrusion detection. For reducing the factor of complexity and consumption of energy a modified Multi-party scheme on computation. K-secure sum protocol was proposed by Sheikh et al [60] that allows multiple cooperating parties for computing function to individual data without data being relieved.

Cluster based private data aggregation (CPDA) uses key distribution in random [61]. The encrypted message prevents from eavesdropping attacks. This method holds three different phases: pre-distribution of key, shared-key discovery and path-key establishment. According to key distribution the phases are classified as cluster formation, calculation of aggregate results among the clusters and data aggregation between clusters.

Privacy Homomorphism (PH) is transformation-based encryption which has an access on direct computation on encrypted data. Initial work on PH was proposed by Rivest and team [62]. In [63] Domingo Ferrer deployed an additive and multiplicative PH which is considered as symmetric scheme and secured against cipher text attacks. This method conceals sensed data end-end and provides effective network data aggregation. The method is further classified into Symmetric and Asymmetric PH scheme.

Data Slicing was introduced and assembled a technique for protecting privacy on data aggregation in WSN. For improving the integrity the author proposed a technique focussing on protecting the integrity of private data-aggregation (iPDA)[64] scheme. This leads to wide number of exchanged messages that creates high communication overhead and computational requirements. Hence these methods have been modified [65-69]. This improves the performance by separating the nodes

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

into leaf and intermediate nodes. Random distribution was introduced for deciding the sliced data to be converted to fixed number.

Conclusion

The methods were classified based on different categories and then different existing methodologies where depicted with their unique functionalities. Privacy preservation data aggregation schemes are also shown that enhances the efficiency of wireless sensor network (WSN). We have listed open scenarios for future research in designing effective protocols for achieving source location privacy.

References

[1] A. Jhumka, M. Leeke, and S. Shrestha, ``On the use of fake sources for source location privacy: Trade-offs between energy and privacy," Comput.J., vol. 54, no. 6, pp. 860874, 2011.

[2] Y. Li, J. Ren, and J.Wu, ``Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans.Parallel Distrib. Syst., vol. 23, no. 7, pp. 13021311, Jul. 2012.

[3] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, ``Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Netw., vol. 7,no. 8, pp. 15011514, 2009.

[4] P. Kamat,Y. Zhang,W. Trappe, and C. Ozturk, ``Enhancing source-location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib.Comput. Syst., Columbus, OH, USA, Nov. 2005, pp. 599-608.

[5] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, “On providing anonymity in wireless sensor networks,” in Parallel and Distributed Systems, 2004. Proceedings. Tenth International Conference on, ser. ICPADS 2004, IEEE. Piscataway, USA: IEEE, 7 2004, pp.411–418.

[6] H. Bahsi and A. Levi, “Energy efficient privacy preserved data gathering in wireless sensor networks having multiple sinks,” in Computer Science and its Applications, 2009. 2nd International Conference on, ser. CSA ’09, IEEE. Piscataway, NJ, USA: IEEE, 12 2009, pp. 1–8.

[7] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, “Temporal privacy in wireless sensor networks,” in 27th International Conference on Distributed Computing Systems, ser. ICDCS 2007, IEEE. Piscataway,USA: IEEE, 6 2007, pp. 23–23.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

[8] N. Li, N. Zhang, S. Das, and B. Thuraisingham, “Privacy preservationin wireless sensor networks: A state-of-the-art survey,” Ad HocNetworks, vol. 7, no. 8, pp. 1501–1514, 11 2009.

[9] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source location privacy in sensor network routing,” in Proc. 25th IEEE International Conference on Distributed Computing Systems, ser. ICDCS 2005, IEEE. Los Alamitos, CA, USA: IEEE Computer Society, 06 2005, pp. 599–608.

[10] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy-constrained sensor network routing,” in Proc. 2nd ACM workshop on Security of Ad hoc and Sensor Networks, ser. SASN ’04, ACM. New York, NY, USA: ACM, 10 2004, pp. 88–93.

[11] K. Mehta, D. Liu, and M. Wright, “Location privacy in sensor networks against a global eavesdropper,” in IEEE International Conference on Network Protocols, ser. ICNP 2007, IEEE. Piscataway, USA: IEEE,10 2007, pp. 314–323.

[12] “Protecting location privacy in sensor networks against a global eavesdropper,” IEEE Trans. Mobile Computing, vol. 11, no. 2, pp. 320–336, 2 2012.

[13] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the ACM, vol. 24, no. 2, pp. 84–90,2 1981.

[14] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy-constrained sensor network routing,” in Proc. 2nd ACM workshop on Security of Ad hoc and Sensor Networks, ser. SASN ’04, ACM.New York, NY, USA: ACM, 10 2004, pp. 88–93.

[15] D. Braginsky and D. Estrin, “Rumor routing algorthim for sensor networks,” in Proc. 1st ACM international workshop on Wireless sensor networks and applications, ser. WSNA ’02, ACM. New York, NY, USA: ACM, 9 2002, pp. 22–31.

[16] Y. Li, L. Lightfoot, and J. Ren, “Routing-based source-location privacy protection in wireless sensor networks,” in Electro/Information Technology, 2009. IEEE International Conference on, ser. EIT ’09, IEEE.Piscataway, NJ, USA: IEEE, 6 2009, pp. 29–34.

[17] J. Yao and G. Wen, “Preserving source-location privacy in energy constrained wireless sensor networks,” in Distributed Computing Systems Workshops, 2008. 28th International Conference on, ser. ICDCS’08, IEEE. Los Alamitos, CA, USA: IEEE Computer Society, 6 2008, pp. 412–416.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

[18] L. Kang, “Protecting location privacy in large-scale wireless sensor networks,” in Communications, 2009. IEEE International Conference on, ser. ICC’09, IEEE. Red Hook, NY, USA: IEEE, 6 2009, pp. 1–6.

[19] P. Spachos, L. Song, and D. Hatzinakos, “Opportunistic routing for enhanced source-location privacy in wireless sensor networks,” in 25th Biennial Symposium on Communications, ser. QBSC 2010, IEEE.Stoughton, WI, USA: The Printing House, Inc., 5 2010, pp. 315–318.

[20] W. Wei-ping, C. Liang, and W. Jian-xin, “A source-location privacy protocol in wsn based on locational angle,” in Communications, 2008.IEEE International Conference on, ser. ICC’08, IEEE. Piscataway,USA: IEEE, 5 2008, pp. 1630–1634.

[21] S. Armenia, G. Morabito, and S. Palazzo, “Analysis of location privacy/energy efficiency tradeoffs in wireless sensor networks,” in Proceedings of the 6th international IFIP-TC6 conference on Ad Hoc and sensor networks, wireless networks, next generation internet, ser. NETWORKING’07, Springer-Verlag. Berlin, Heidelberg: Springer-Verlag, 5 2007, pp. 215–226.

[22] X. Luo, X. Ji, and M. Park, “Location privacy against traffic analysis attacks in wireless sensor networks,” in Information Science and Applications International Conference on, ser. ICISA 2010, IEEE. Piscataway, NJ, USA: IEEE, 4 2010, pp. 1–6.

[23] L. Zhang, “A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing,” in Proc. 2006 international conference on Wireless communications and mobile computing, ser. IWCMC ’06, ACM. New York, NY, USA: ACM, 7 2006, pp. 33–38.

[24] I. Shaikh, H. Jameel, B. dAuriol, H. Lee, S. Lee, and Y.-J. Song, “Achieving network level privacy in wireless sensor networks,” Sensors, vol. 10, no. 3, pp. 1447–1472, 8 2010.

[25] L. Lightfoot, Y. Li, and J. Ren, “Preserving source-location privacy in wireless sensor network using star routing,” in 2010 IEEE Global Telecommunications Conference, ser. GLOBECOM 2010, IEEE. Piscataway,USA: IEEE communications society, 12 2010, pp. 1–5.

[26] X. Hong, P. Wang, J. Kong, Q. Zheng et al., “Effective probabilistic approach protecting sensor traffic,” in Military Communications Conference,2005. IEEE, ser. MILCOM 2005, IEEE. Piscataway, NJ,USA: IEEE, 10 2005, pp. 169–175.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

[27] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, “Temporal privacy in wireless sensor networks,” in 27th International Conference on Distributed Computing Systems, ser. ICDCS 2007, IEEE. Piscataway,USA: IEEE, 6 2007, pp. 23–23.

[28] M. Mahmoud and X. Shen, “A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10,pp. 1805–1818, 10 2012.

[29] H. Chen and W. Lou, “From nowhere to somewhere: protecting endto- end location privacy in wireless sensor networks,” in Performance Computing and Communications Conference, IEEE 29th International,ser. IPCCC 2010. Piscataway, USA: IEEE, 12 2010, pp. 1–8.

[30] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in The 27th Conference on Computer Communications, ser. INFOCOM 2008, IEEE. Piscataway,USA: IEEE, 4 2008, pp. 51–55.

[31] Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, “Source location privacy against laptop-class attacks in sensor networks,” in SECURECOM:Proc. 4th international conference on Security and privacy in communication netowrks, ser. SecureComm ’08, ACM. New York,NY, USA: ACM, 9 2008, pp. 5:1–5:10.

[32] X. Luo, X. Ji, and M. Park, “Location privacy against traffic analysis attacks in wireless sensor networks,” in Information Science and Applications International Conference on, ser. ICISA 2010, IEEE.Piscataway, NJ, USA: IEEE, 4 2010, pp. 1–6.

[33] J. Sheu, J. Jiang, and C. Tu, “Anonymous path routing in wireless sensor networks,” in Communications, 2008. IEEE International Conference on, ser. ICC’08, IEEE. Piscataway, USA: IEEE, 5 2008, pp.2728–2734.

[34] S. Misra and G. Xue, “Efficient anonymity schemes for clustered wireless sensor networks,” International J. Sensor Networks, vol. 1,no. 1, pp. 50–63, 1 2006.

[35] A. Nezhada and A. Dimitris Makrakis, “Location privacy and anonymity preserving routing for wireless sensor networks,” Computer Networks, vol. 52, no. 18, pp. 3433–3452, 12 2008.

 https://doi.org/10.37896/pd91.4/91473

[36] L. Grieco, G. Boggia, S. Sicari, and P. Colombo, “Secure wireless multimedia sensor networks: a survey,” in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2009. Third International Conference on, ser. UBICOMM’09, IEEE. Los Alamitos, CA, USA:IEEE Computer Society, 10 2009, pp. 194–201

[37] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta,“Cross-layer enhanced source location privacy in sensor networks,” in Proc. 6th Annual IEEE communications society conference on Sensor,Mesh and Ad Hoc Communications and Networks, ser. SECON’09,IEEE. Piscataway, NJ, USA: IEEE Press, 6 2009, pp. 324–332.

[38] N. Dutta, A. Saxena, and S. Chellappan, “Defending wireless sensor networks against adversarial localization,” in Proc. 2010 Eleventh International Conference on Mobile Data Management, ser. MDM 2010, IEEE. Los Alamitos, CA, USA: IEEE Computer Society, 2010,pp. 336–341.

[39] R. Rios and J. Lopez, “Exploiting context-awareness to enhance source-location privacy in wireless sensor networks,” The ComputerJournal, vol. 54, no. 10, pp. 1603–1615, 6 2011.

[40] R. El-Badry, M. Youssef, and A. Sultan, “Hidden anchor: Providing physical layer location privacy in hybrid wireless sensor networks,” in Proc. 3rd international conference on New technologies, mobility and security, ser. NTMS’09. Piscataway, NJ, USA: IEEE Press, 5 2009,pp. 254–258.

[41] B. Tavli, M. Ozciloglu, and K. Bicakci, “Mitigation of compromising privacy by transmission range control in wireless sensor networks,”IEEE Commun. Lett., vol. 14, no. 12, pp. 1104–1106, 10 2010.

[42] S. Oh and M. Gruteser, “Multi-node coordinated jamming for location privacy protection,” in Military Communications Conference, 2011, ser. MILCOM 2011, IEEE. Piscataway, NJ, USA: IEEE, 11 2011, pp.1243–1249.

[43] JUN LONG, MIANXIONG DONG, KAORU OTA, AND ANFENG LIU, “Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks” , Volume 2 2014.

[44] Bidi Ying1,2, Dimitrios Makrakis1, Hussein T. Mouftah, “A Protocol for Sink Location Privacy Protection in Wireless Sensor Networks, IEEE Globecom 2011 proceedings.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

[45] Yun Li Jian Li Jian Ren, “Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks”, 31st annual conference , IEEE International Conference on Computer Communication.

[46] Yun Li, Jian Ren,” Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks” , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 7, JULY 2012.

[47] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, “The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012.

[48] Abdel-shakour Abuzneid, Tarek Sobh, and Miad Faezipour, “An Enhanced Communication Protocol for Anonymity and Location Privacy in WSN”, 2015 IEEE Wireless Communications and Networking Conference (WCNC) - Workshop - Energy Efficiency in the Internet of Things for Energy Efficiency.

[49] Abhishek R. Malviya, Balaso N. Jagdale, “Location Privacy of Multiple Sink Using Zone Partitioning Approach in WSN”, 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

[50] Daojing He1, Jiajun Bu1, Sencun Zhu2, Mingjian Yin1, Yi Gao1, “Distributed Privacy-Preserving Access Control in a Single-owner Multi-user Sensor Network”, Mini-Conference at IEEE INFOCOM 2011.

[51] Neelanjana Dutta, Abhinav Saxena and Sriram Chellappan, “DefendingWireless Sensor Networks Against Adversarial Localization”, Eleventh International Conference on Mobile Data Management.

[52] Petros Spachos, Liang Song, and Dimitrios Hatzinakos, “Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks”, 25th Biennial Symposium on Communications.

[53] Jian Ren Yun Li Tongtong Li, “Routing-Based Source-Location Privacy in Wireless Sensor Networks”, IEEE ICC 2009 proceedings.

[54] BISTA R, YOO H K, CHANG J W. A new sensitive data aggregation scheme for protecting integrity in wireless sensor networks[C]// Proceedings of 10th IEEE International Conference on Computer and Information Technology, 2010:

 https://doi.org/10.37896/pd91.4/91473

[55] BLA E-O, ZITTERBART M. An efficient key establishment scheme for secure aggregating sensor networks[C]//Proceedings of the 1st ACM Symposium on Information, Computer and Communications Security, 2006:303 – 310.

[56] BUTZ A R. Alternative algorithm for Hilbert's space filling curve[J]. IEEE Transactions on Computers,1971,20(4):424–426.

[57] KIM Y, LEE H, YOON M, et al. Hilbert-Curve Based Data Aggregation Scheme to Enforce Data Privacy and Data Integrity for Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2013, Article ID 217876, 14 pages.

[58] PANTHACHAI Y, KEERATIWINTAKORN P. An energy model for transmission in Telos-based wireless sensor networks[C] // Proceedings of the International Joint Conference on Computer Science and Software Engineering (JCSSE '07),2007.

[59] SHEIKH R, KUMMAR B, MISHRA D. Privacy preserving k secure sum protocol[J]. International Journal of Computer Science and Information Security, 2009,6(2):184-188

[60] HE Wenbo, LIU Xue, Nguyen H, *et al.* Pda: Privacy- preserving data aggregation in wireless sensor networks[C]// Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM'07). 2007:2045–2053.

[61] LAURENT E, GLIGOR D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security,2002:41–47.

[62] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J].Foundations of Secure Computation (Academic Press, New York), 1978:169-179.

[63] FERRER J D. A new privacy homomorphism and applications[J]. Information Processing Letters,1996,60(5):277- 282.

[64] HE Wenbo, Nguyen H, LIU Xue, et al. iPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks[C]//Proceedings of the IEEE Military Communications Conference,2008:1-7.

[65] LI Hongjuan, LIN Kai, LI Keqiu. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks[J]. Computer Communications,2011,34(4):591–597.

 https://doi.org/10.37896/pd91.4/91473

[66] LIU Chenxu, LIU Yun, ZHANG Zhenjian, et al. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks[J]. International Journal of Communication Systems,2013,34(26):380-394.

[67] YANG Geng, LI Seng, XU Xiaolong, et al. Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2013, Article ID427275, 12 pages.

[68] SHI Jing, ZHANG Rui, LIU Yunzhong, et al. Pri-Sense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems[C]//Proceedings of the 29th Conference on Computer Communications (INFOCOM '2010), 2010:1-9.

[69] WILSON R, ROSEN P. Protecting Data through 'Perturbation' Techniques: The Impact on Knowledge Discovery in Databases[J]. Journal of Database Management, 2003,14(2):14-26.

[70] X. Luo, X. Ji, and M. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in Information Science and Applications International Conference on, ser. ICISA 2010, IEEE.Piscataway, NJ, USA: IEEE, 4 2010, pp. 1–6.

[71] J. Sheu, J. Jiang, and C. Tu, "Anonymous path routing in wireless sensor networks," in Communications, 2008. IEEE International Conference on, ser. ICC'08, IEEE. Piscataway, USA: IEEE, 5 2008, pp.2728–2734.

[72] A. Nezhada and A. Dimitris Makrakis, "Location privacy and anonymity preserving routing for wireless sensor networks," Computer Networks, vol. 52, no. 18, pp. 3433–3452, 12 2008.

[73] J. Chen, X. Du, and B. Fang, "An efficient anonymous communication protocol for wireless sensor networks," Wireless Communications and Mobile Computing, vol. 12, no. 14, pp. 1302–1312, 10 2011.

[74] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, and F. Makedon, "Providing anonymity in wireless sensor networks," in Pervasive Services, IEEE International Conference on, ser. ICPS 2007, IEEE. Washington, DC, USA: IEEE Computer Society Press, 7 2007,pp. 145–148.

[75] R. Di Pietro and A. Viejo, "Location privacy and resilience in wireless sensor networks querying," Computer Communications, vol. 34, no. 3, pp. 515–523, 3 2011.

 https://doi.org/10.37896/pd91.4/91473

ISSN: 0369-8963

[76] J. Park, Y. Jung, H. Ko, J. Kim, and M. Jun, “A privacy technique for providing anonymity to sensor nodes in a sensor network,” in Ubiquitous Computing and Multimedia Applications, Second International Conference, ser. UCMA 2011, SERSC. Berlin Heidelberg, Germany: Springer, 4 2011, pp. 327–335.

[77] S. Misra and G. Xue, “Efficient anonymity schemes for clustered wireless sensor networks,” International J. Sensor Networks, vol. 1,no. 1, pp. 50–63, 1 2006.

 https://doi.org/10.37896/pd91.4/91473