Int. J. Nonlinear Anal. Appl. 14 (2023) 1, 2111–2121
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.6785

Spatio temporal based distributed message and source location security protocol to wireless sensor network-polynomial based scheme

Parthasaradhi Mayasala[a,*], S. Murali Krishna[b,*]

[a]SVCE, JNTUA Anantapuramu, India
[b]SV College of Engineering, Tirupati, India

(Communicated by Madjid Eshaghi Gordji)

Abstract

Message and node authentication is one among the foremost effective ways to prevent nodes from being propagated, forwarded, and corrupted, unauthorized messages over wireless sensor networks (WSNs). In order to alleviate those challenges, several message authentication schemes based on symmetric or public key cryptosystems have been developed. Despite various benefits, many challenges still exist in the attack mitigating in the wireless sensor network such as considering the reputation of a source and updating it dynamically by considering node transmission characteristics on packet data with the source and intermediate node acts neighbour. In addition, most of them have the constants of communication overhead, high computations, resilience and scalability. To address these issues, a novel polynomial-based scheme has been developed and it has been named Spatial Temporal based Distributed Message and Source Security Authentication Protocol. However, this scheme address all the weakness of built-in threshold-based schemes employed for message authentication in determining the degree of the polynomial. The puzzle-based node authentication has been enabled for intermediate nodes; the proposed scheme allows unlimited message transmission by any node without the struggling problem of the threshold.

Keywords: Source Location Privacy, Hop by Hop Encryption, Wireless Sensor Network, Energy Efficient Technique, Channel Allocation and Migration, Energy Conservation, Bandwidth Efficiency
2020 MSC: 68N30

1 Introduction

Nowadays, wireless sensor networks are being used in various applications such as animal monitoring, weather forecasting, healthcare, monitoring transport, military and so on. Wireless sensors are designed to capture relevant events and collected data is sent to the base station through the network (event trigged transmission)[1]. The events have three parameters, event description, time, and location.

Wireless sensor networks are implemented in environments where the wired network setup is too difficult. So, they have numerous security threats such as node compromise, routing disruption and false data injection. Among these

*Corresponding author
Email addresses: urssaradhi@gmail.com (Parthasaradhi Mayasala), muralikrishna.s@svcolleges.edu.in (S. Murali Krishna)

Received: December 2021 *Accepted:* June 2022

threats source location, and privacy are more different because it has not been addressed using security mechanisms like authentication and encryption. That means that the description of event transmission is accomplished via encryption [3, 10], but the event location and time cannot be achieved via cryptographic [4, 18]. Therefore, providing privacy for the location of the source sensor and events reported by them by an attacker is known as source anonymity or source location privacy (SLP).

Privacy problem in wireless sensor networks is broadly classified into two categories [5]: User-centric privacy and Network centric privacy, as shown in Fig.1.

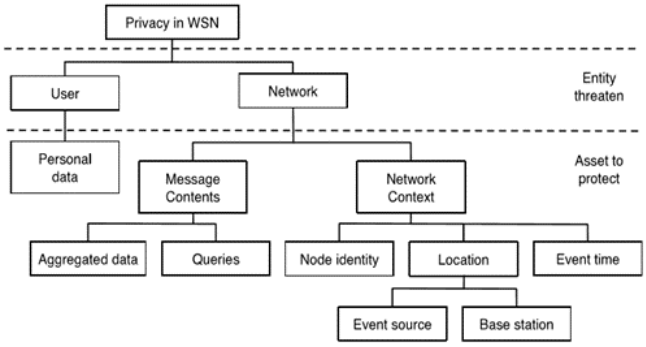

Figure 1: Categories of Privacy in WSN [5].

Different techniques are proposed to deal with source location privacy but the problem is resource consumption is too high with these approaches which cause less network lifetime. To increase the network lifetime with location privacy we are proposing Spatio temporal-based distributed message and source location security protocol to wireless Sensor Network- Polynomial Based Scheme.

NS-2 simulator is used to conduct the tests, which are then verified using a variety of criteria. As for the rest, it's categorised as follows: related work of Section II. Section III explains assumed models for the work. Section IV explains the proposed protocol Spatio temporal-based distributed message and source location security protocol to wireless Sensor Network in detail. Section V details the testing of the suggested technique using various metrics. Finally, Section VI provides the scientific contribution of the study to future research.

2 Related Work

There are many approaches to the problem of Source Location Privacy and message privacy on the inclusion of path Allocation and traffic scheduling in the Wireless Sensor Network. The Approaches are as follows:

The source location privacy schemes are proposed under the attacker who is external, passive, local and global. Therefore, to enhance the privacy of the source location different techniques are proposed. These techniques are described under three types of attackers: Local, Global attacker and Distributed eavesdropping attacker.

2.1 Techniques under Local attacker

The local attacker has limited mobility and partial view of the network traffic. In the view of local attackers, routing-based techniques are proposed to provide source location privacy. These techniques are baseline routing techniques (single path routing and flooding-based routing, flooding with fake messages proposed by C.Ozturk et al. [13]. In which fake messages are generated even more no real event. Phantom routing proposed by P.Kamat et al.[7], which is a combination of random walking and flooding. GROW proposed by Y.Xi et al. [19], which is a two-way random walk. Path perturbation algorithm proposed by Hoh et al. [6], which is applied to monitor the patients health and cyclic entrapment method. Ouyang et al.[12], proposed CEM which is a looping method where attackers are trapped. A cross-layer solution was proposed by M.Shao et al. [15], which has two phases MAC layer broadcast and routing. Wang et al. [20], proposed privacy-aware routing has two techniques RP routing, and WRS routing. Rios et al. [14] had proposed CALP in which routing tables of the nodes are updated after a message transmission. W.Tan et al. [18], proposed PEM in which fake messages are generated when real messages are transmitted.

2.2 Techniques under Global attacker

In the view of a global attacker, the routing-based techniques are ineffective, because the global attacker has the entire view of network traffic and immediately detects the time and location of the event trigged transmission. K.Mehta et al. [11], propose periodic collection in which a real message is forwarded when timer trigged if the node has a message in the queue, otherwise sends a fake message. Shao et al.[16], proposed a fit probe rate scheme which increases the latency of the messages. Yang et al.[21], proposed event Source Un-observability which is an inclusion of PFS and TFS. Li et al.[8], proposed Source location privacy through RRIN and NMR. Alomair et al. [2], proposed interval indistinguishability in which real messages are transmitted without waiting for the trigged timer. Spachos et al. [17], proposed ADRS in which messages are transmitted based on the angle of the receiver. Zhou et al. [22], proposed a method for preserving location privacy from global attackers hiding under the FOG.

3 ASSUMED MODELS FOR WORK

In this section, we describe the assumption models of networks and attackers, which are used in this paper.

3.1 Preliminaries of the Proposed architecture

Message authentication: A node is capable to verify that the received message is sent by a node either declared or specific nodes in a particular cluster. In other words, an attacker is unable to locate a false node and can't inject fake messages into the network.

Message integrity: A node is capable to verify that the received message has been modified by the attackers. In other words, the attackers are unable to modify the content of the message by performing any message detection techniques.

Identity and location privacy: The attackers cannot identify the location and ID of the source by analyzing the network traffic.

Node compromise resilience: The network should be resistant to node compromise attacks. No matter how many nodes are threatened, the remaining nodes are still safe.

3.2 Network Model -Wireless Sensor Network

The wireless sensor network has a group of sensors with a unique address. This entire network is divided into regions with regional heads. Each region is again divided into clusters based on the fastest message delivery ratio. Each cluster is identified using a unique address. Every cluster has a special node known as a cluster head. Cluster head has the special features for long life existence and it has the capabilities of communicating with all the sensors and with base station either single or multi-hop channel. All the sensor nodes within a cluster are directly or indirectly communicated with the cluster head and vice versa. The cluster heads which are nearer to the base station are directly communicated with it and the cluster heads which are far from the base station are communicated through the regional heads. Routing of the data towards the base station can be employed using a graph model which helps to create a routing table with dynamic updates easily. The below two diagrams are depicting the communication of the sensors with the base station.

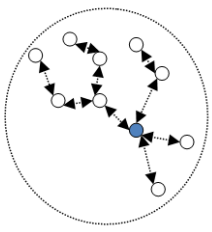

Figure 2: Individual Sensor Communicating with Cluster Heads

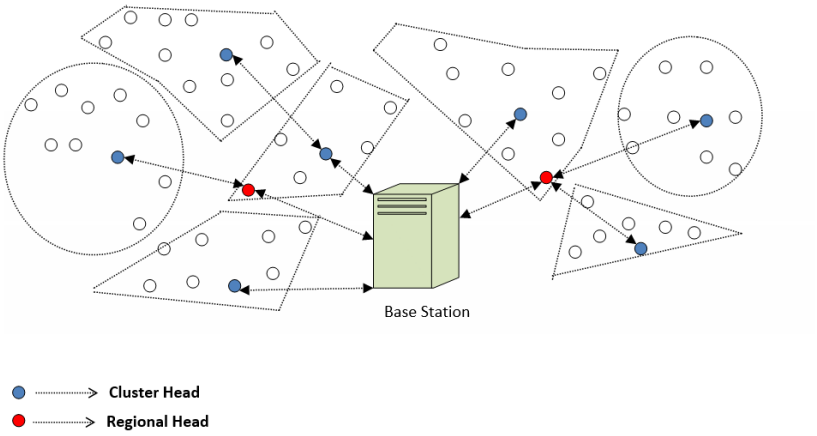

Figure 3: Cluster Heads communicating with Base Station

3.3 Deriving Attack characteristic for node controlling and packet modification

In this model, attacking nature has been extracted and it is simulated to control the attack propagation in the network using Node Controlling Attack and Packet Modification Attack. In Controlling Attack, an attacker can make a sensor function abnormally. In a packet modification attack, an attacker can modify the message contents.

4 Proposed Model -Spatial Temporal based Distributed Message and Source Security Authentication Protocol

In this section, Spatial-Temporal based Distributed Message and Source Security Authentication Protocol which extends the Source location privacy protocol was discussed as it is composed of a polynomial regression scheme which provides thresholding values for the nodes, Message Security based on ELGamal scheme provides message authentication, Level based Non-Disclosure Differential privacy provides source privacy and Puzzle based Node Authentication which is to provide network resilient architecture against the propagation of attacks.

4.1 Modelling polynomial Regression scheme based on thresholding

In this, a polynomial is related to data transfers by nodes on the specified flow of packets. The intermediate nodes verify the authenticity of the message through a polynomial regression evaluation. The polynomial evaluation is carried out on node density, no of successful data transmission, request cancellation and rate of data transfer. The node will be considered for transmission if it meets any of the specified limits on the above-mentioned criteria. Utilizing criteria is considered a threshold. The importance of this mechanism is to determine nodes with high bandwidth and to provide the category of the node in terms of levels.

Ni denotes the set of the node
Node density Means Available Bandwidth
Node degree means available bandwidth slots
Exchange Hello Message between the one hops neighbour nodes
Set Suitable node = 0
Calculate Node Density N^d
For (i=0 to N)
Set Nd Max = Threshold
If (N_i^d >= N^d Max)
Set N_i^d as Node Density
Else
Check next node
Calculate Node Degree N^r

For (i=0 to N)
Set N^r Max = Threshold
If ($N_i{}^r$ >= N^r Max)
Set $N_i{}^r$ as Suitable Node on Node degree
Else
Check next node
Calculate Quality Range of Node ()
Data transfer D= x
Successful of data transfer = y
Q= Percentage (y/x)
If (Q > 75)
Quality Range is high
Else
Quality Range is Low
Compute level ()
If (Node with high density && Node with High quality)
Set particular Node as suitable node
Update the Suitable node ()
Suitable Node = Suitable Node +1
Set level ()
If (quality of suitable node[i] == Max && Node Density of suitable node[i] == Max)
Level of suitable node[i] = high
Else
Level of suitable node[i] = low
Else
Prioritize based on other condition

Algorithm 1: Polynomial regression scheme for Thresholding

Certificate revocation List (CRL) Checking

On the computation of the node characteristics, the trust certificates of the attacking node have to be revoked by the issuing Certificate Authority. Revocation is the process of invalidating a node. Other nodes should be able to detect that the certificate is revoked in a timely manner and prevent users from further scheduling packets. It helps in mitigating the attacking node by utilizing only the CRL.

4.2 Modelling Elliptic-curve cryptography algorithm for Message Security based on ELGamal scheme

An alternative solution is proposed to prevent the intruder from recovering the polynomial by calculating the coefficients of the polynomial. The idea is to add random noise to the polynomial, also called a disturbance factor, so that the coefficients of the polynomial are not easy to solve. However, a recent study showed that error-correcting code techniques can be used to completely remove random noise from polynomials.

In public key methods, the digital signature is added to the message using a private key of the sender. All intermediate nodes and final receiving nodes verify the received message using a public key of the sender. High computational overhead is one of the limitations of public key methods. The overhead is caused due to cypher text generation. The overhead computation is as follows:

$$LBF = \frac{n_c}{\sum_i (x_i - \mu)^2},$$

LBF - Load balancing factor, where n_c is number of packet to be transmitted, x_i is the data cardinality, μ is the average of number of neighbors of a data transmission for message.

To avoid more communication cot and delay, updates are periodically gathered by data of the intermediate. Public-key cryptography is primarily based totally on the intractability of positive mathematical problems. Early public-key structures are stable assuming that it's miles tough to thing of a massive integer composed of or greater massive top factors. For elliptic-curve-primarily based totally protocols, it's miles assumed that locating the discrete logarithm of a random elliptic curve detail with recognition to a publicly recognized base factor is infeasible — that is the "elliptic curve discrete logarithm problem" or ECDLP. The complete protection of Elliptic-curve cryptography relies upon at

the capacity to compute a factor multiplication and the incapacity to compute the multiplicand given the authentic and product points. The problem difficulty is determined by the elliptic curve size. The size of the elliptic curve is determined as follows:

$$R_{i,j} = \lambda_{i,j} B_j.$$

In ECC, the size of the key is very smaller and it requires less space which is suitable for wireless sensor networks to increase the lifetime of the network with a lower transmission rate.

4.3 Developing the Source Privacy and Eliminating the Encrypted Message traces –Level based Non-Disclosure Differential privacy

In order to protect the location information and compressed encrypted message traces of the source, anonymous intermediate node selection strategies have been devised in this section. The node selection strategies eliminate the adversaries from obtaining message and location information on the analysis of routing information. It has been achieved by developing a Level based Non- disclosure differential privacy mechanism based on the level of the node determined by the polynomial regression scheme in the above section.

Generate Tree structure for the Suitable node
Generate pseudonym (Suitable Node)
Tree (Suitable Node ())
If (level of node[i] = high)
Provide Location information to the intermediate
Else

Algorithm 2: Level based non-disclosure differential privacy (LNDP scheme)

Raise the request to revert the false information of the source to the Intermediate node. The source location will be transmitted on basis of the level of the node which is considered a strategy of disclosure of the information. In this location and message, traces can be preserved easily from an adversary. It is considered a lightweight model privacy model as it is easily distinguishing the node based on the level. In addition, it creates sufficient diversity so that it is infeasible for the adversary to find the message source.

The flowing diagram for the Level based non-disclosure differential privacy is illustrated in below Figure 4.

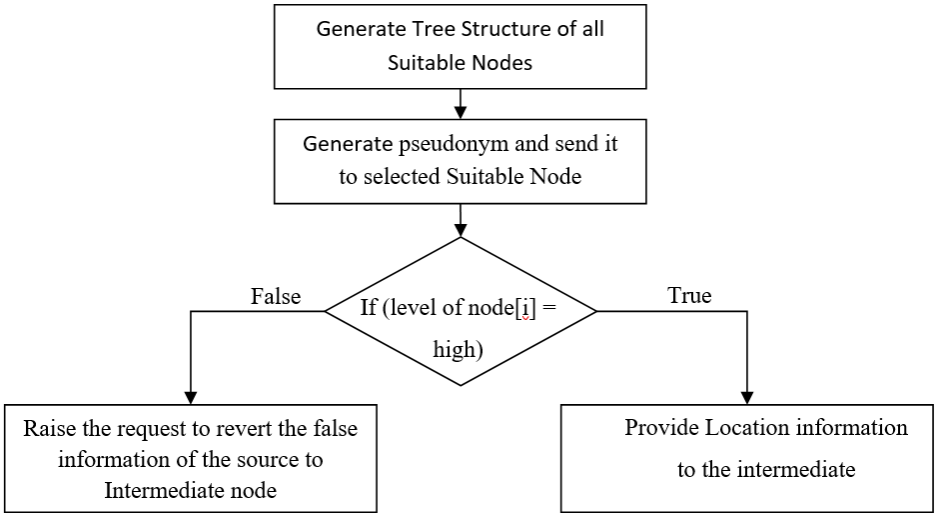

Figure 4: Level based non-disclosure differential privacy (LNDP scheme)

4.4 Puzzle based Node Authentication

The node authentication is a primary constraint in the attack propagation network as it leads to eavesdropping and packet classification attacks during data transmission even after strong encapsulation of location and message authentication mechanisms. In this part, a puzzle-based node verification mechanism has been employed to verify the

node behaviour on transmitting the data. In this algorithm, node information is transferred to a neighbour node after verification of the puzzle. The mechanism works in terms of puzzles; before extracting the message the receiver has to solve the puzzle within a stipulated time. A puzzle can take any form of computation based on the medium of usage. The puzzle generator function generates a cryptogram puzzle and it is added to the message then it is transmitted.

Algorithm
Sender Perceptive:
Create a cipher text for the message C=E(M)
Generate a jigsaw puzzle P using Puzzle_Generator function with time T.
SM = C + P
Transmit the SM
Receiver Perceptive
Receive SM
Solve the Puzzle with in a Stipulated Time T.
If Puzzle Solved then
M = D(C)
Else:
Discard the SM without Decrypting

5 Simulation results

The network setup in simulation is described in below table 1.

Table 1: Parameters for Simulation

Simulation Parameter	Value
Simulator	NS2
Topology Size	1000m *1000m
Number of Nodes	200
Transmission Power	0.5mW/Hz
Channel Width	5,10,15,20 MHz
Bandwidth of the Network	2Mbps
Traffic type	CBR
Pause Time	10s,20s
Data Packet size	512 bytes
Buffer size	100 packets
Simulation Time	30 minutes

The following figures represents that our proposed protocol STDMSS is better than the existing protocol Dark-Light Stripe Alternation (DLSA) in different aspects.

5.1 Energy Efficient

Energy utilization of in STDMSS and DLSA is shown in figure-4.

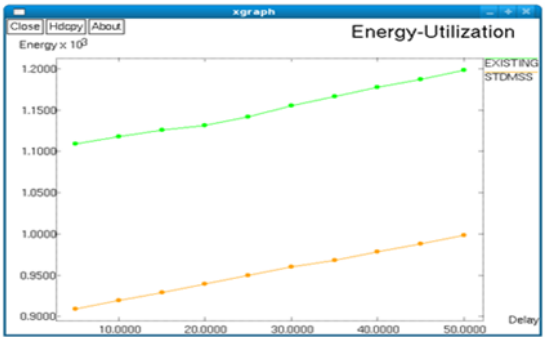

Figure 5: Energy Efficient in STDMSS and DLSA

5.2 Throughput

Throughput of in STDMSS and DLSA is shown in figure-5.

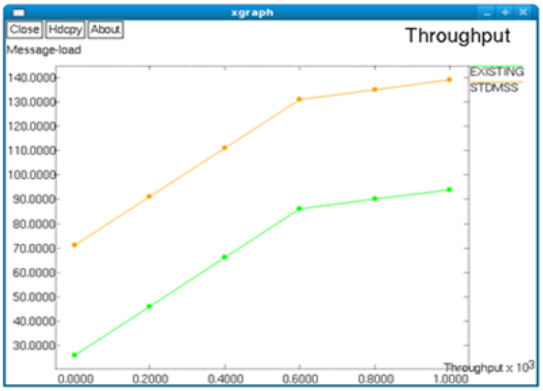

Figure 6: Throughput in STDMSS and DLSA

5.3 Routing Overhead

Routing overhead of in STDMSS and DLSA is shown in figure-4.

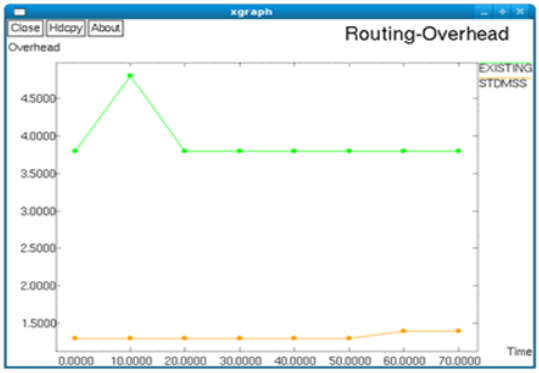

Figure 7: Routing Overhead in STDMSS and DLSA

5.4 Packet Delivery Ratio

Packet Delivery Ratio of in STDMSS and DLSA is shown in figure-4.

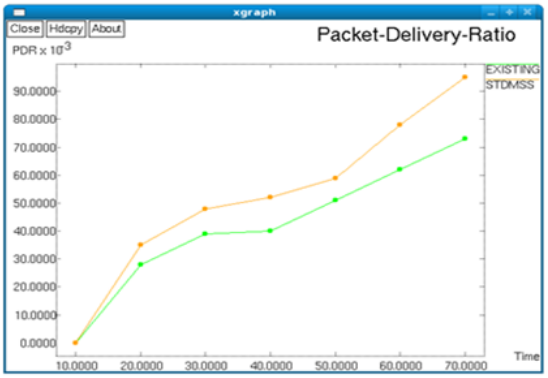

Figure 8: Packet Delivery Ratio in STDMSS and DLSA

5.5 Routing Latency

Routing Latency of in STDMSS and DLSA is shown in figure-4.

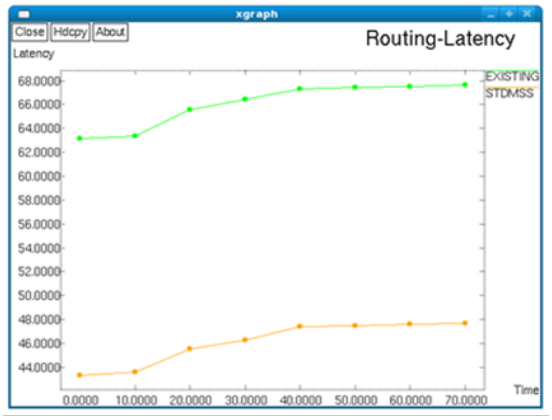

Figure 9: Routing Latency in STDMSS and DLSA

Table 2: Performance Evaluation of DLSA and STDMSS

Technique	**Throughput in mbps**	**Overhead in mbps**	**Packet Delivery Ratio**	**Energy Utilization in m/Hz**	**Routing Latency**
Dark-Light Stripe Alternation - Existing	75.58	10.23	95.78	0.7	0.35
Spatial Temporal Distributed Message and Source Security Protocol- Proposed	79.26	12.59	99.85	0.9	0.25

6 Conclusion

We designed and simulated the proposed spatial Temporal based distributed message and source secure authentication protocol using NS2 Simulator towards achieving both attack resilience and energy utilization in terms of bandwidth management. The Proposed protocol extends the Hop by Hop Authentication protocol through encapsulation of source privacy (packet header) on the proposed model and the proposed protocol proves that it is better than the existing protocol. In future work, a novel node scheduling method can be employed to reduce the energy and delay of broadcasting nodes in networks.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, *Wireless sensor networks: A survey*, J. Comput. Networks **38** (2002), no. 4, 393–422.

[2] B. Alomair, A. Clark, J. Cuellar and P. Radha. *Toward a statistical framework for source anonymity in sensor networks*, IEEE Trans. Mobile Comput. **12** (2013), no. 2, 248–260.

[3] M. Mathapati, T.S. Kumaran, K.H. Prasad and K. Patil, *Framework with temporal attribute for secure data aggregation in sensor network*, SN Appl. Sci. **2** (2020), no. 12, 1–10.

[4] L. Gao and X. Wang, *A game approach for multi-channel allocation in multi-hop wireless networks*, Proc. 9th ACM Int. Symp. Mobile Ad Hoc Network. Comput., 2008, pp. 303—312.

[5] G. Han, X. Miao, H. Wang, M. Guizani and W. Zhang, *CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks*, IEEE Trans. Vehicular Technol. **68** (2019), no. 3, 2739–2750.

[6] B. Hoh and M. Gruteser, *Protecting location privacy through path confusion*, Proc. IEEE/CreatNet First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), Athens, 2005, pp. 194–205.

[7] P. Kamat, Y. Zhang, W. Trappe and C. Ozturk, *Enhancing source-location privacy in sensor network routing*, Proc. IEEE 25th Int'l Conf. Distributed Comput. Syst.(ICDCS '05), Washington DC, 2005, pp. 599–608.

[8] Y. Li and J. Ren, *Preserving source-location privacy in wireless sensor networks*, 6th Ann. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks. IEEE, 2009, pp. 493–501.

[9] J. Lopez, R. Rios, B. Feng and G. Wang, *Evolving privacy: From sensors to the internet of things*, Future Gen. Comput. Syst. **75** (2017), 46–57.

[10] M.M.E.A. Mahmoud and X. Shen, *A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks*, IEEE Trans. Paral. Distributed Syst. **23** (2012), no. 10, 1805–1818.

[11] K. Mehta, D. Liu and M. Wright, *Location pPrivacy in sensor networks against a global eavesdropper*, 15th IEEE Int. Conf. Network Protocols–ICNP'07, Beijing, 2007, pp. 314–323.

[12] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon and U. Lowell, *Entrapping adversaries for source protection in sensor networks*, Proc. IEEE Seventh Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WOWMOM '06), Buffalo-Niagara Falls, 2006, pp. 32–41.

[13] C. Ozturk, Y. Zhang and W. Trappe, *Source-location privacy in energy-constrained sensor network routing*, Proc. Second ACM Workshop Security of Ad Hoc Sensor Networks (SASN '04), ACM New York, Washington DC, 2004, pp. 88–93.

[14] R. Rios and J. Lopez, *Exploiting context-awareness to enhance source-location privacy in wireless sensor networks*, Comput. J. **54** (2014), no. 10, 1603–1615.

[15] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy and T. La Porta, *Cross-layer enhanced source location privacy in sensor networks*, Proc. IEEE Comm. Soc. Sixth Ann. Conf. Sensor, Mesh Ad Hoc Comm. and Networks (SECON '09), Rome, 2009, pp. 1–9.

[16] M. Shao, Y. Yang, S. Zhu and G. Cao, *Towards statistically strong source anonymity for sensor networks*, 27th Conf. Comput. Commun. INFOCOM'08, Phoenix, 2008, pp. 466–474.

[17] P. Spachos, D. Toumpakaris and D. Hatzinakos, *Angle-based dynamic routing scheme for source location privacy in wireless sensor networks*, IEEE 79th Vehicular Technol. Conf. (VTC Spring), Seoul, 2014, pp. 1–5.

[18] W. Tan, K. Xu and D. Wang, *An anti-tracking source location privacy protection in WSN based on path extension*, IEEE Internet Things J. **1** (2014), no. 5, 461–471.

[19] Y. Xi, L. Schwiebert and W. Shi, *Preserving source location privacy in monitoring-based wireless sensor networks*, Proc. IEEE 20th Int'l Parallel & Distributed Process. Symp. (IPDPS '06), 2006, pp. 1–8.

[20] H. Wang, B. Sheng and Q. Li, *Privacy-Aware Routing in Sensor Networks*, J. Computer Networks **53** (2009), no. 9, 1512–1529.

[21] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar and G. Cao, *Towards event sSource unobservability with minimum*

network traffic in sSensor networks, Proc. First ACM Conf. Wireless Network Secur. (WiSec '08), ACM New York, , 2008, pp. 77–88.

[22] Q. Zhou and X. Qin, *Preserving source location privacy against the global attacker hiding in FOG*, in IEEE-ICNSC, 2018, pp. 1–6