Volume 64, Issue 1, 2020
Journal of Scientific Research
Institute of Science,
Banaras Hindu University, Varanasi, India.

Context Oriented Source Location Privacy Protection Techniques for Event Monitoring Wireless Sensor Networks

Nisha[*1], S. Suresh[1]

[1]Department of Computer Science, Banaras Hindu University, Varanasi.
nishasngh703@gmail.com, suresh.selvam@bhu.ac.in

Abstract: **Location privacy is one of the most challenging threats that has grown to acquire attention across the globe. Wireless sensor network (WSN) where the transmission occurs through multiple hops between the nodes suffers from attacks such as backtracking and directional attacks by the adversaries. As an analogy, sensor nodes employed in wildlife monitoring region to constantly monitor their presence and activities are threatened by attackers. The attackers constantly monitor the transmission with the objective of locating the source node ultimately leading to poaching. In order to do away with these threats leading to location disclosure, various routing mechanisms that involves phantom node, fake packets and fake source nodes have been proposed time and then by various researchers. In this paper we present a comprehensive study of various routing mechanisms for source location privacy preservation that are compared on four parameters: i. safety period ii. energy consumption iii. Packet latency iv. Network life time. Different routing mechanisms are analyzed in detail and future scope for improvement is provided to enhance further research.**

Index Terms: **Adversaries, fake source, phantom nodes, source location privacy, shortest path transmission.**

I. INTRODUCTION

Recently, WSN (Akyildiz et al., 2002; Kim et al., 2017) has found its immense use in many fields including military, environment, personal and many others (Bushnag et al., 2018). Wireless sensor network defines the network to be consisting of very small sensor nodes which facilitate the transmission of data through multi hops from a particular sensor node (source) to a destination. The capacity of node depends on the resources (processor, memory, etc.) that it is built with and lifetime of the sensor node depends on the amount of energy that consumes during transmission. The sensor nodes are capable of sensing the environment (e. g. presence or movement of objects). They are employed to sense for and then send the information in the form of packets to the base station where it is processed further. The base station keeps a record about each and every data or information it receives from the sensor nodes.

Protection of data is a critical issue and has been an active area of research (Yao et al., 2013; Chow et al., 2009). Numerous approaches have been proposed and implemented including various routing and encryption techniques (Karimi & Kalantari, 2018; Xie & Wang, 2016) in order to prevent the data leakage to the adversaries. Adversaries are the ones who attack the network when the data is being transmitted. They might try to corrupt the intermediate nodes to trace the information flow or introduce a large number of fake packets to block the routing process or induce an attack on the sink to directly gain the information. For example: in wildlife conservation, the sensor nodes are deployed with the objective of detecting an animal and informing the sink about the location of the animal. There may be adversaries as hunters who constantly monitor the transmission and try to get the location of the animal further putting a threat on the life of the animal.

Location privacy protection (Akyildiz et al., 2002; Kim et al., 2017; Zhou et al., 2014) is divided into two categories: i. Source location protection ii. Sink location protection. Source location protection deals with securing the location of the source node whereas sink location protection deals with securing the location of the sink from the attacks by the adversaries. In other words, both the source and sink location protection techniques are prolongs the location inference by adversaries with only contextual information. This paper provides a detailed analysis of various routing strategies employed for source location privacy protection against various types of adversaries. Sink

DOI: http://dx.doi.org/10.37398/JSR.2020.640145

location privacy is out of scope of this paper, however interested readers can refer to (Yao et al., 2013; Chai et al., 2012; Ngai et al., 2013; Chen et al., 2014,2016; Liu et al. 2017) for more information.

The rest of this paper is organized as follows: Section II describes the background consisting of network model and adversary model. Section II represents the analysis and detailed discussion of source location privacy mechanisms and Section IV provides a comparative study of various source location protection techniques. Finally, the conclusion and future research direction is presented to encourage further research.

II. BACKGROUND

Source location privacy protection techniques have been discussed exclusively since last two decades. Several routing mechanisms like flooding (Ozturk et al., 2004; Kamat et al., 2005), phantom routing flooding (Ozturk et al., 2004; Kamat et al., 2005; Yao et al., 2015), fake packet injection (Bushnag et al., 2018; Ren et al., 2013) and various others have been proposed to fulfill the objective of securing the source. However, it is very important to understand that performance should be very high for any mechanism to be considered efficient and applicable in real applications. Most of the existing solutions are designed by assuming a particular network model and provides privacy against a particular adversary model(s).

A. Network model

To ensure privacy against adversaries, the deployment and interaction between sensor nodes should be in a proper manner. The sensor nodes can be deployed in a random or according to a particular architecture that further affects the efficiency of nodes and performance of the technique as a whole. Network model is defined by the following features:

- Deployment of the sensor nodes is either structured or unstructured depending on the architecture of the network.
- The sensor nodes have a finite memory and certain amount of energy and the nodes remain alive and functional as long as the node does not run out of energy.
- The nodes may be rechargeable by attaching solar cells but in most of the cases it is not rechargeable which means once the provided energy is over, the nodes can take part in no transmission.
- There might be one or more than one sink available which is responsible for keeping a record of all the information received over the time and it is assumed to have infinite energy and memory space.
- The network area is divided into grids, rings or clusters on the basis of the routing technique to be used.

B. Adversary model

The disclosure of information by adversary during wireless transmission of packets is a major concern for location privacy. Adversaries are broadly divided into two categories:

i. Local adversaries (Zhou et al., 2014; Bushnag et al., 2018): These adversaries have very limited network devices to track and thus are less capable. Their scope of monitoring or carrying out any kind of attacks on the network is limited.
ii. Global adversaries (Mehta et al., 2007; Ren et al., 2013): These are stronger in terms of capability than local adversaries. They are very well equipped with tracking devices and can monitor the entire network transmission.

The attacks by either local or global adversary can be divided into two categories:

i. Content oriented attacks: These type of attacks means alterations to the actual content while on their routing path or by corrupted nodes and thus these altered content provide false information to the sink.
ii. Context oriented attacks: These type of attacks do not have to deal with any alterations to the content rather route blocking, injecting traffic, exhausting node's energy etc. are employed in order to obtain the location information.

On the basis of nature of the attack, it can further be categorized into two:

i. Active attack: It deals with attack on the nodes or by the nodes which means that it includes attacks by the corrupted/malicious nodes on the dedicated ones. In this type of attack, the adversary can even alter the contents or block the route of packets etc.
ii. Passive attacks: It deals with no attacks on the nodes rather includes back tracking, eaves dropping, traffic monitoring and others.

Fig.1. provides a clear categorization of the adversarial model.

III. SOURCE LOCATION PRIVACY (SLP) MECHANISMS

This section describes the popular mechanisms developed for securing location of the source in detail. Source location privacy was first modelled by Ozturk et al. (2004) as a Panda-Hunter game model where the hunter was assigned the task of finding the panda whose location was being hidden. In this work, the authors compared various routing algorithms and provided with a new idea of phantom flooding. A detailed description of baseline flooding (Groschupp, 2017), probabilistic flooding (Jeong et al., 2012; Groschupp, 2017) and flooding with fake messages was laid followed by phantom flooding. Baseline flooding states that each and every node forwards the packet only one time and if the node has already forwarded a packet once, it will refrain from sending the same packet to any

neighbor node again. In probabilistic flooding, the decision whether the node that received a packet will transmit (forward) the packet to its neighbor node or not depends on the probability that it generates which is compared against an already specified probability. Flooding with fake messages deals with setting up a persistent or non-persistent fake source which would continuously send fake messages to divert the adversary. All the above three mechanisms were simulated and compared with respect to safety time, energy consumption and packet latency and probabilistic flooding was found to be better among all the three. Phantom flooding was based on probabilistic flooding and it comprised of two steps: one is random walk (Tian et al., 2006) and the second is flooding, preferably probabilistic flooding. The packets are first transmitted in random walk or a directed random walk to a phantom node and then through probabilistic flooding the packets are transmitted to sink. The performance of the proposed mechanism depicted in Fig. 2 was found better than the existing techniques in terms of safety period and energy consumption.

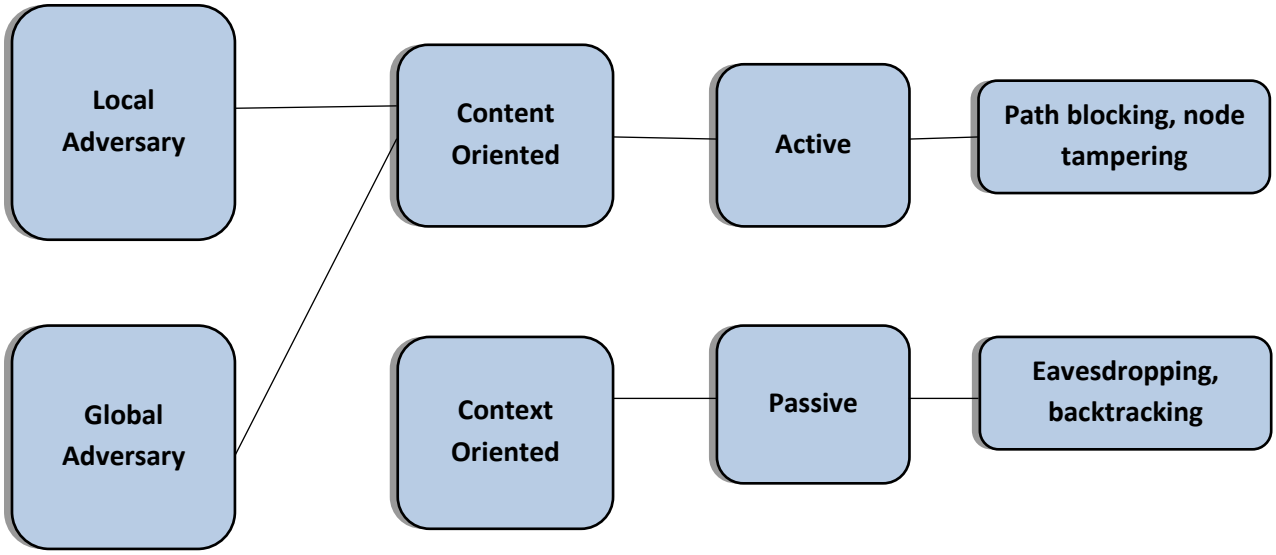

Fig. 1. Adversary Model

By improving phantom flooding, a new mechanism termed as phantom routing was proposed by Kamat et al. (2005). The author pointed out that there is always a trade-off between the privacy and energy consumption of nodes and any mechanism that provides location privacy should also minimize the energy consumption and in this context phantom routing proved to be balancing both the parameters in a much efficient way. As similar to phantom flooding, phantom routing was composed of two steps: one is random or directed random walk of packets to a phantom source and the second step is flooding or single path routing of packets from phantom node to sink. Random walk or random directed walk in the first step was again narrowed down to choice between sector based random walk or hop based random walk from source to the phantom node. After the first phase, most preferably a shortest path routing was adopted to deliver the packets to the sink. This mechanism increased the privacy without incurring greater energy consumption as compared to other mechanisms.

Jiang et al. (2018) proposed another approach for location privacy where the transmission was divided in two phases against local adversary. In the first phase, the source sends the packet to an intermediate node after which, in the second phase, the intermediate node follows shortest path routing to sink. The first phase where the source sends a packet to the specific intermediate node follows a distribution method to estimate the probability of the neighboring nodes among which the one having the highest probability is chosen as the next node to transmit the packet. Most preferably the nodes which are closer to the source have the highest probability to which packet can be transmitted. Since the nodes have no location based device to locate their location, they use the hop count in order to determine the probability. After the packet reaches the intermediate node, it follows the shortest path route to finally deliver it to sink. The performance of this mechanism was measured in terms of path ratio, energy ratio and safety period. Path ratio measures the delay of packet from source to sink whereas energy ratio is the ratio between the number of messages that are routed in the entire network to the number of messages that follows the shortest path and safety period is measured by number of packets that a source can send before the adversary finally attains its position.

Routing strategy based on sectors to provide source location privacy was proposed by He et al. (2019) where the strategy named Sector based Random Routing (SRR) dealt with dividing the network in various sectors and then performing the routing as per the proposed strategy. In SRR, first of all the network is divided into a specific number of sectors and annular rings are established with sink at the center. The routing process starts

with source sending the packet that contains an extra information of attached angle to an intermediate node that lies outside the visible region. After the intermediate node receives the packet, it transmits the packet in the annular ring till a specific node attains that angle and that specific node is termed as a phantom node. Phantom node is responsible for transmitting the packet to sink through random routing. The author has further specified that this scheme is resistant to attacks such as directional attack and backtrack attack. The SRR routing process is represented in Fig.3.

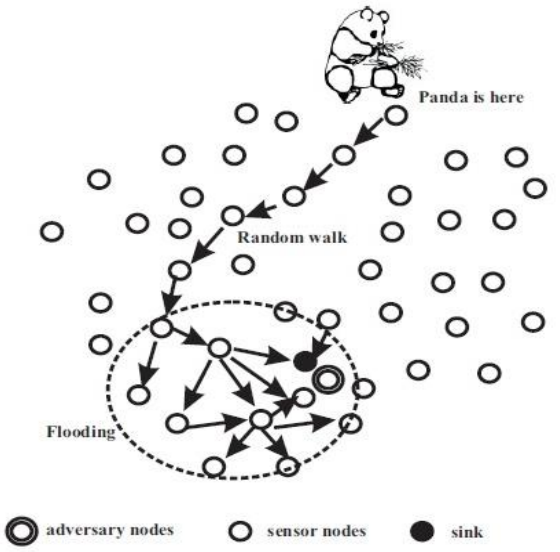

Fig. 2. Phantom flooding (Ozturk et al., 2004)

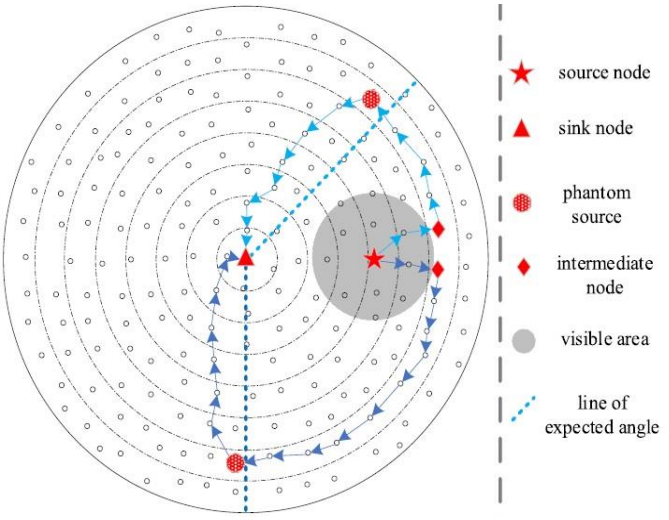

Fig. 3. Representation of SRR Mechanism (He et al., 2019)

A tree based diversionary approach has also been suggested for securing location information by Long et al. (2014). This new mechanism is termed as Tree Route (TR) and it needs to operate through two phases. The first phase is about constructing a backbone routing through the edge of the network consisting of diversionary routes to the phantom nodes and the second phase is about establishing diversionary routes from the diversionary routes set up in first phase as many as possible. In the routing process as shown in Fig. 4, the background route consists of nodes which act as intermediate nodes from which diversionary routes to the network edges are constructed. These network edges consist of phantom nodes which transmit dummy packets to the intermediate nodes at each interval. If there is any real event occurring, the phantom nodes near the source node would transmit it to intermediate node from where it is transmitted to the sink. TR succeeded in achieving a better lifetime and security level.

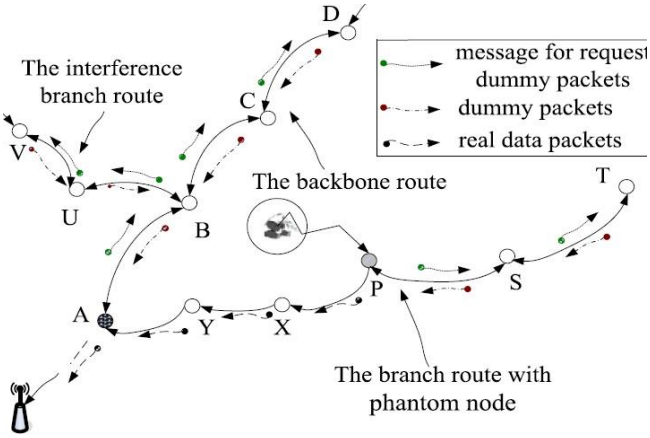

Fig.4. Representation of TR Mechanism (Long et al., 2014)

Location based services (LBS) (Anwar et al., 2013; Chow et al., 2009) are very common in today's world which are very frequent in use by various applications for various purposes. But use of LBS can also affect the location privacy of users as data regarding the location can be somehow obtained by adversaries. K-anonymity (Gedik & Liu, 2007) is a mechanism developed to protect the context data from being leaked or interpreted by the unauthorized ones. K-anonymity specifies that the location information of a single mobile user sent to LBS for its services must remain anonymous to LBS with at least k-1 other mobile users. The author designed a perturbation engine to anonymize the location information with k-1 other mobile clients and the engine that consists of numerous spatio-temporal cloaking algorithms [10] as its working core. The proposed mechanism provided high quality of service when implemented in real life situations.

Jayanthi et al. (2019) gave a new direction to anonymity by proposing improvement in all direction random routing (ARR) technique by injecting fake packets as well as inclusion of random walk of packets. This technique deals with anonymizing both source and sink nodes. An anonymous region is constructed near source and sink and packets are transmitted from fake source to fake sink in order to hide the location of actual source. The actual source randomly routes the packet to its neighbor which further routes it randomly to its neighbors and when it reaches the sink, the sink decrypts it using a secret key attaining the location of the source. The number of fake sources injecting

fake packets in network and fake sinks performing decryption is all determined on the basis of traffic flow.

All the above techniques were employed to safeguard the context information from local adversaries having limited view and capabilities, but what if the adversaries are global who have better tracking devices and higher capabilities. In such a case, the techniques for protecting source location information should be far more strong and efficient. Mehta et al. (2007) proposed periodic collection and source simulation in order to secure the location data from global eavesdropper. In periodic collection mechanism, every sensor node sends a dummy packet to the sink at regular interval. Every sensor node consists of queue which stores the packet in FIFO manner and it transmits the contents of queue every 't' seconds. The queue stores the real packets if the node senses any event otherwise stores the dummy packets and transmits at each 't' seconds to neighbor nodes. The real packets are authenticated and accepted for further transmission by the next hop nodes and dummy ones are rejected. The queue size limits the size of data packets that can be transmitted. This technique leads to very high energy consumption as all the sensor nodes have to transmit packets at regular intervals. To reduce the energy consumption, source simulation technique was proposed. In this technique, a set of virtual nodes are selected to simulate the transmission of the real source node. In each round, the selected nodes transmit fake packets to the base station, hiding the source node sending the actual packet. This technique reduced the energy consumption and provided less communication overhead as compared to existing techniques.

Another approach for providing source location privacy against global adversaries was provided by Ren et al. (2013) who proposed a cyclic diversionary routing in interference rings for transmission purpose. In this mechanism, first of all the network is divided into number of rings consisting of sensors of respective hop counts and further within each ring, the nodes are divided into number of clusters where each cluster contains a clusterhead. A set of rings based on their probability is selected as interference rings to follow a cyclic diversionary routing and the ring where the event occurred is also selected to perform cyclic diversionary routing.

At each periodic interval, the nodes of the interference rings start sending dummy packets to each of their cluster heads and all the cluster heads that receive dummy packets will discard the packets and only that cluster head which receives the real event packet will keep that packet. A promoter (node) is selected from among the cluster heads in the outermost ring which passes a dummy packet to the closest cluster head of the next inner ring. If the inner ring is an interference ring, selected based on the probability, then the packet transmission takes place one full cyclic route. After it completes a complete cycle, it is then passed to the nearest cluster head of the inner ring. When it reaches the event ring, the dummy packet travels in a cyclic manner and it gets replaced with real event packet as soon as it reaches the cluster head holding the real packet. Following the above strategy, the real packet is delivered to the sink. A clear view of routing through CDR is provided in Fig.5. Though the energy consumption was higher, this mechanism provides higher safety time.

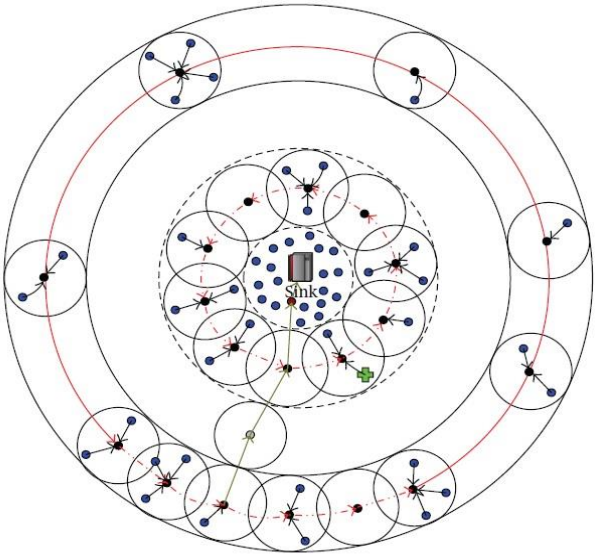

Fig.5. Representation of CDR Mechanism (Ren et al.,2013)

In multiring routing mechanism suggested by Yao et al. (2015), the author proposed the use of multiple rings to achieve the context security. According to the proposed mechanism, the network is divided into number of rings based on the hop counts of nodes and then for each node three lists containing far, equal and near neighbor nodes is maintained. The source node sends the packet to an intermediate node in the outer ring and after it reaches to the intermediate ring it covers a specific angle within that ring. After covering that specified angle in the outer ring, it is directed to a specific inner ring where it again travels a specific angle according to the criteria set by the mechanism. And then finally it is transmitted to the sink through shortest path routing. Both the angles that the packet covers in outer and inner ring should be equal to 180 degrees. In the mean time of the routing process, the neighbor nodes also inject fake packets to divert the adversary, thus improving the safety period.

IV. COMPARISON.

From the literature study, we observe that among diverse mechanisms, incorporation of fake packets was employed in most of them. Fake packets are introduced in the network in order to have diverse transmission paths of packets. This would lead the adversary away from the actual transmission of event packet, ultimately increasing the safety time. It is clear that the introduction of fake packets in the network though improves privacy, but leads to more traffic in the network and higher energy consumption. And higher energy consumption ultimately lowers network lifetime. In order to further secure the source,

ring routing mechanisms were proposed in which transmission of packets, be it dummy or event packets, occur in a cyclic fashion. This causes a cyclic entrapment of adversaries and increases the safety period of the mechanism. But, on observation we can find that even in this mechanism, the energy consumption is very high as a lot of nodes are involved in transmission.

Even the type of adversary i.e. local or global adversary plays an important role in determining the efficiency of certain mechanism. Some mechanisms might provide very high security against local adversary but they might just fail in case the adversary is global. But for mechanisms that provide good security against global adversary works extremely well against local adversary.

However, we provide an analysis of efficiency for each of the mechanisms. The table. 1 represents a comparative view of different mechanisms discussed in this paper along four parameters i. safety period ii. energy consumption iii. packet latency iv. network lifetime.

Table -1: Comparative view of the SLP Mechanisms

Papers/Author	**Mechanism**	**Adversary**	**Safety period**	**Energy consumption**	**Packet latency**	**Network life time**
Ozturk et al., (2004)	Phantom flooding	Local	High	Moderate	High	Moderate
Kamat et al., (2005)	Phantom routing	Local	High	Low	Low	High
Jiang et al., (2018)	Probabilistic distribution	Local	Moderate	Low	Moderate	Moderate
He et al., (2019)	Sector based Random routing	Local	High	Moderate	Moderate	High
Long et al., (2014)	Tree based diversionary path	Local	High	High	Low	High
Gedik et al., (2007)	k- anonymity	Local	Moderate	Low	Moderate	Moderate
Jayanthi et al., (2019)	All direction random routing	Local	Moderate	High	High	Low
Mehta et al., (2007)	Periodic collection (PC)& source simulation(SS)	Global	PC: Moderate SS: Moderate	PC: High SS: Lower	PC: High SS: Lower	PC: Low SS: Moderate
Ren et al., (2013)	Cyclic diversionary routing	Global	High	High	Moderate	Moderate
Yao et al., (2015)	Randomized angle based routing	Local	Moderate	High	Moderate	Low

CONCLUSION AND FUTURE DIRECTIONS

Source location privacy is increasingly becoming crucial with advancing technology and advanced threats that need to be thwarted. Location privacy mechanisms have to be constantly improved in order to provide security since the attackers are constantly trying to break the privacy mechanism in one or the other way. This paper has provided an insight into some of the most famous and strong source location privacy preservation mechanism against both local and global adversaries. Since the performance of the privacy mechanisms is measured under safety period, energy consumption, packet latency and network lifetime, a detailed comparative description and analysis for each of the mechanisms has been provided based on these four parameters.

However, as for future directions, it must be noted that strength of any mechanism lies equally on safety period, packet latency and network lifetime which must be optimized. Routing mechanisms must be developed having higher safety time, higher network lifetime and not incurring any communication overhead.

REFERENCES

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications magazine, 40(8), 102-114.

Anwar, M., Masoumzadeh, A., & Joshi, J. (2013). 1 Security and Privacy in. Advanced Location-Based Technologies and Services, 235.

Bushnag, A., Abuzneid, A., & Mahmood, A. (2018). Source anonymity against global adversary in wsns using dummy packet injections: A survey. Electronics, 7(10), 250.

Chai, G., Xu, M., Xu, W., & Lin, Z. (2012). Enhancing sink-location privacy in wireless sensor networks through k-anonymity. International Journal of Distributed Sensor Networks, 8(4), 648058.

Chen, J., Lin, Z., Liu, Y., Hu, Y., & Du, X. (2016). Sink location protection protocols based on packet sending rate adjustment. International Journal of Distributed Sensor Networks, 12(1), 6354514

Chen, J., Zhang, H., Du, X., Fang, B., & Yan, L. (2014). Designing robust routing protocols to protect base stations in wireless sensor networks. Wireless Communications and Mobile Computing, 14(17), 1613-1626.

Chow, C. Y., & Mokbel, M. F. (2009). Privacy in location-based services: a system architecture perspective. Sigspatial Special, 1(2), 23-27.

Gedik, B., & Liu, L. (2007). Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing, 7(1), 1-18.

Groschupp, F. (2017). Location Privacy Preserving Mechanisms. Network, 9.

He, Y., Han, G., Wang, H., Ansere, J. A., & Zhang, W. (2019). A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things. Future Generation Computer Systems, 96, 438-448.

Jayanthi, R. & Mohanraj, M.. (2019). An Anonymity Region Construction and Two Fold Location Protection Scheme for Improving Source and Sink Location Privacy in WSN. International Journal of Computer Sciences and Engineering. 7. 724-730. 10.26438/ijcse/v7i2.724730.

Jeong, H., Jeong, H., & Yoo, Y. (2012, February). Dynamic probabilistic flooding algorithm based-on neighbor information in wireless sensor networks. In The International Conference on Information Network 2012 (pp. 340-345). IEEE.

Jiang, S., Li, M., & Tang, Z. (2018). A New Scheme for Source-location Privacy in Wireless Sensor Networks. IJ Network Security, 20(5), 879-889.

Kamat, P., Zhang, Y., Trappe, W., & Ozturk, C. (2005, June). Enhancing source-location privacy in sensor network routing. In 25th IEEE international conference on distributed computing systems (ICDCS'05) (pp. 599-608). IEEE.

Karimi, R., & Kalantari, M. (2011, August). Enhancing security and confidentiality in location-based data encryption algorithms. In Fourth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2011) (pp. 30-35). IEEE.

Kim, B. S., Park, H., Kim, K. H., Godfrey, D., & Kim, K. I. (2017). A survey on real-time communications in wireless sensor networks. Wireless communications and mobile computing, 2017.

Liu, A., Liu, X., Tang, Z., Yang, L. T., & Shao, Z. (2017). Preserving smart sink-location privacy with delay guaranteed routing scheme for WSNs. ACM Transactions on Embedded Computing Systems (TECS), 16(3), 1-25.

Long, J., Dong, M., Ota, K., & Liu, A. (2014). Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. IEEE Access, 2, 633-651.

Mehta, K., Liu, D., & Wright, M. (2007, October). Location privacy in sensor networks against a global eavesdropper. In 2007 IEEE International Conference on Network Protocols (pp. 314-323). IEEE

Ngai, E. C. H., & Rodhe, I. (2013). On providing location privacy for mobile sinks in wireless sensor networks. Wireless networks, 19(1), 115-130.

Ozturk, C., Zhang, Y., & Trappe, W. (2004, October). Source-location privacy in energy-constrained sensor network routing. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 88-93).

Ren, J., Zhang, Y., & Liu, K. (2013). An energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks. International Journal of Distributed Sensor Networks, 9(4), 834245.

Tian, H., Shen, H., & Matsuzawa, T. (2006). Random walk routing in WSNs with regular topologies. Journal of Computer Science and Technology, 21(4), 496-502.

Xie, Q., & Wang, L. (2016). Privacy-preserving location-based service scheme for mobile sensing data. Sensors, 16(12).

Yao, L., Kang, L., Deng, F., Deng, J., & Wu, G. (2015). Protecting source–location privacy based on multirings in wireless sensor networks. Concurrency and Computation: Practice and Experience, 27(15), 3863-3876.

Yao, L., Kang, L., Shang, P., & Wu, G. (2013). Protecting the sink location privacy in wireless sensor networks. Personal and Ubiquitous Computing, 17(5), 883-893.

Zhou, L., Wan, C., Huang, J., Pei, B., & Chen, C. (2014, November). The location privacy of wireless sensor networks: Attacks and countermeasures. In 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 64-71). IEEE.

***