International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Framework for Enhancing Source Location Privacy in Wireless Sensor Networks

Parthasaradhi M[1], B Nagalakshmi[2], D Venkatesh[3]

[1]PG Student, Dept. of CSE, Gates Institute of Technology, Gooty, Anantapur, A.P., India

[2]Associate Professor in Department of CSE, Gates Institute of Technology, Gooty, Anantapur, A.P., India

[3]Professor and Dean, Department of CSE & IT, Gates Institute of Technology, Gooty, Anantapur, A.P., India

Abstract: ***As sensor network applications become integrated into our lives, as we know that when the sensor networks are deploys untrustworthy environments, where the problem is privacy for source location and events reported by sensor nodes. This problem is called source anonymity problem in wireless sensor networks. Based on different adversarial assumptions different techniques were 9proposed for it. In this paper we consider source anonymity against global attacker. Unfortunately it is very difficult and expensive to achieve. Because of through traffic analysis attackers may attack on privacy of source sensor and also sensor networks are limited in resources. In this work we propose a formal frame work for modeling the anonymity in sensor networks. The proposed model contains twofold: First, it introduces "interval in distinguish ability", that provides a quantitative measure to source anonymity. The significance of interval indistinguishability is that it prevents a source information leakage that can't be captured using existing models and it determines the quantity of anonymity of current designs. Second, distributed fake traffic allocation algorithm which embedding the real message into the chosen fake message to hide the real message. We assumed fixed amount of resources to fake messages and we try to share it among the sensors to maximize the degree of anonymity of the system.***

Keywords: Wireless sensor network, location privacy, source anonymity, event-trigged transmission, interval indistinguishability.

1. Introduction

A wireless sensor network is a group of sensor nodes, which designed to capture the relevant events and collected data is send through the network to a main location. This type of transmission of data is called event-trigged transmission. The types of the events detected by the sensor nodes are dependent on the application. The applications are transport monitoring, military use, weather forecasting, healthcare, animal monitoring and so on [3], [4].

Wireless sensor networks are also constructed with many security threats such as node compromise, routing disruption and false data injection. Because of they are normally implemented in environments where it is difficult to setup wired networks. Among all of these threats, source location privacy is special interest since it cannot be fully addressed by security mechanisms such as encryption and authentication. Consider an example; the sensor networks are implemented in animal monitoring system, is illustrated in Figure 1. When sensor detects an event; it is sends a message includes description, time and location of event to base station. If an attacker can hack this message, he can take some action to capture or kill the animal.

The events have the three parameters, 1) The event description, 2) The event time and 3) The event location. When the wireless sensor networks are deployed in animal monitoring or untrustworthy environments, the three parameters of events plays an important security feature in the design of wireless sensor networks. The transmission of event description can be achieved via encryption primitives [5]-[8], but the time and location of events cannot be achieved via cryptographic [9], [10].

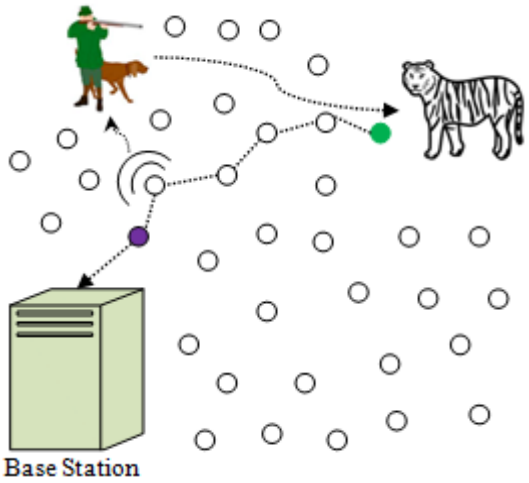

Figure 1: An application of sensor networks for animal monitoring

The problem of studying techniques that provide time and location privacy for events reported by sensor nodes is called source anonymity problem in wireless sensor networks. The source anonymity problem has been raising topic in wireless sensor networks [9]-[19].

In the existing literature the source anonymity problem has been described in two types of attackers. First, a local attacker, how have the limited mobility and partial view of the network traffic. To achieve source location privacy in the view of local attacker routing based techniques have been proposed [11]-[15]. Second, the global attacker, how is able to monitor the entire

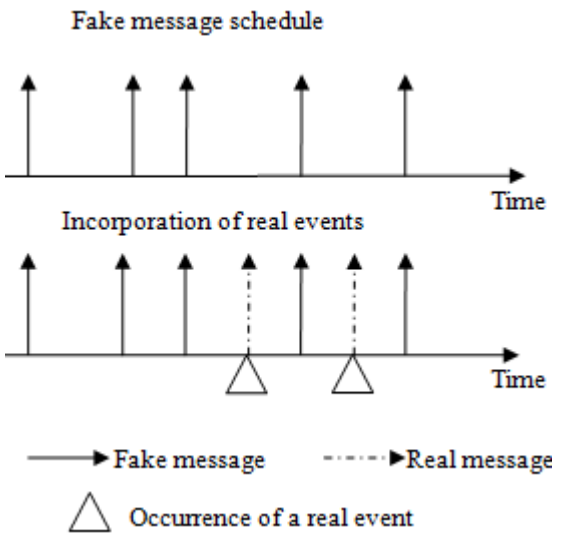

Figure 2: An illustration of the intuitive approach. The node is programmed to transmit fake messages so that real events are hidden within the fake transmissions.

network traffic. The routing-based techniques are ineffective in the view of global attacker. Because of global attacker have the entire view of a network; it can immediately detect the time and location of the event-triggered transmission.

An approach to send an event without leaking to a global attacker is that, the nodes are design to transmit fake events even if no real events are reported. When the real events as soon as they can be transmitted. This approach does not completely solve the source location privacy problem. Because of the fake transmissions are scheduled according to the probabilistic distribution of time. The attacker can use the statistical analysis to distinguish between the fake and real transmissions, if real events are transmitted as they captured. This approach is illustrated in Figure 2.

One way to solve this problem is illustrated in Figure 3. When real events occur, they can be transmitted instead of the next scheduled fake transmission. For example, nodes are programmed to transmit encrypted messages every minute. If there is no real event to report, the node transmits fake message. When a real event occurs, it must be delayed until the next scheduled fake transmission before it can be sent out.

2. Assumed models for work

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

2.1 Network Model

We assume that, in a network communication will be done by the sensors nodes. The sensor nodes are assumed as, it contains unchangeable batteries, and thus the designs of this type of nodes are requirement. The nodes are programmed to transmit fake messages even if there is no real message occurred. If real message occurs, the nodes sent real messages including within the transmissions of fake messages. The nodes also contains security encryption algorithm. So that attackers cannot differentiate between the transmission of real and fake messages by using cryptographic test. When a node captures an event, it places information about the event in a message and sends it in an encrypted format.

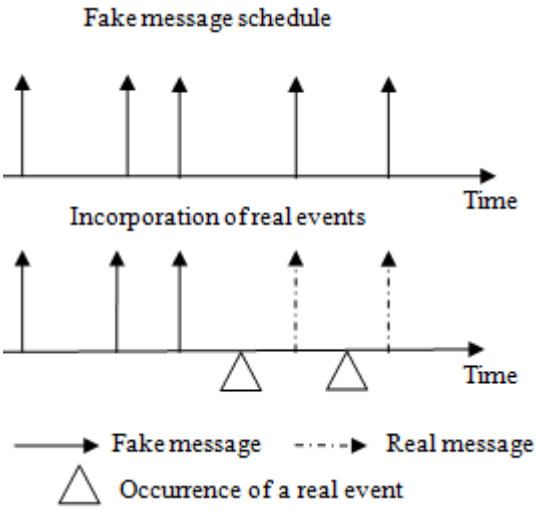

Figure 3: An illustration of the solution. Nodes are programmed to transmit fake messages according to some pre-defined probabilistic distribution. When a real event occurs, it must be delayed until the next scheduled fake transmission before it can be sent out.

2.2 Attacker's model

The attacker model is similar to the one considered in [9], [10], in that it is external, passive and global. The external attacker does not control the nodes in the network and also has no control over the real event process. The passive attacker has the capability of observing the network traffic. The global attacker can monitor the entire network and can observe the timing and origin of every transmitted message.
The attacker assumed as, how knows the locations of all nodes in the network, also assumed to know the distribution of fake message transmissions. Assumed as, the attacker had the capability of observing nodes transmissions over extended periods of times. And the attacker cannot break the security of the encryption algorithm and differentiate the report of event via cryptographic tests.

3. Proposed Frame Work

In this section, we introduce our frame work of source anonymity model for wireless sensor networks.

3.1 Interval Indistinguishability

The main goal of source location privacy is to hide the existence of real messages from the attackers. This implies that, an attacker observing a sensor node during extended period of time, in which some of the intervals include the transmission of real messages and others do not. The attackers must not be able to determine the intervals that contain real messages with significant confidence. This leads to the notion of interval indistinguishability that can be defined as

Definition1 (Interval Indistinguishability):
Let I_f denotes a time interval, called fake interval that contains fake event transmissions, I_r denotes a time interval called real interval that contains real event transmissions. The two time intervals are said to be statistically indistinguishable, in the distribution of inter-transmission times during these two intervals should not be distinguished by means of statistical tests.

3.2 Modeling Interval indistinguishability

To model interval indistinguishability, we propose the following game between the system designer C (Challenger) and an attacker A.

Game 1:

1) C chooses two intervals I_f and I_r, in which I_f denotes fake interval and I_r denotes real interval.
2) C draws a bit b from the set {0, 1} and sets $I_r = I_0$ and $I_f = I_1$.
3) C gives I_0 and I_1 to attacker A.
4) A will makes any statistical test on I_0 and I_1 and outputs a bit b'
5) If $b' = b$, then A wins the game.

From the definition indistinguishability and game 1, we need to find a security measure that can be quantifying the source anonymity of different systems. Let $\Pr[b' = b]_\sigma$ be the attacker's probability of winning game 1 using a strategy σ to identifying the real interval. We quantify the source anonymity of the sensor network by

$$\Lambda_\sigma = 1 - 2(\Pr[b' = b] - 0.5) \quad (1)$$

In the best case, the attackers strategy is a pure random guess, i.e., $\Pr[b' = b]_\sigma = \frac{1}{2}$ and $\Lambda_\sigma = 1$, then we get absolute anonymity. In the worst case, $\Pr[b' = b]_\sigma = 1$ and $\Lambda_\sigma = 0$ leads to no anonymity. The best strategy will result probability of winning the game to the interval [0.5, 1], leading to the source anonymity measure in the interval [0,1].

Let $\sum$ be the set of all possible attacker strategies to attack the system. Then, the anonymity of the system is,

$$\Lambda = \min_{\sigma \in \sum} \Lambda_\sigma \quad (2)$$

Where Λ_σ is as defined in the equation (1).
Now, we are introducing the notion of Λ- anonymity in sensor networks from the definition1.

Definition 2:

A wireless sensor network is said to be Λ- anonymity if it satisfies two conditions.

1. An interval beginning and ending cannot be distinguishable.
2. The anonymity of the system is at least Λ, as defined in equation (2).

In definition 2, the first condition says that there is a transition region between intervals that cannot be distinguishable. If such a transition exists, then that leads to anonymity breach.

3.3 Distributed fake traffic allocation algorithm

Let x_i denotes the allocated resource for sending fake messages from sensor node i, λ_i is an average rate of transmitting a fake message by a sensor node i. C is the total rate of fake traffics, i.e. the maximum affordable cost for sending fake traffic, Where

$$\sum_{i=1}^{N} x_i \le C \quad (3)$$

And

$$\lambda = \sum_{i=1}^{N} \lambda_i \quad (4)$$

$X = (x_1, \ldots, x_N)$ is the vector representation of fake traffics, and let μ denotes the probabilistic distribution time (mean time) to transmit a fake message. To establish a fake traffic in entire network for each step each value of μ and x_i of sensor i will be updated. Precisely speaking, in the k^{th} iteration step, $\mu^{(k)}$ and $x_i^{(k)}$ is updated as follows;

$$\mu^{(k+1)} = \left[\mu^{(k)} + \gamma\left(\sum_{i=1}^{N} x_i^{(k)} - C\right)\right]^+ \quad (5)$$

$$x_i^{(k+1)} = (\lambda + C)2^{-(\log_2^{\xi} + \mu^{(k)})} - \lambda_i \quad (6)$$

where

$$0 < \gamma < \frac{2}{\ln 2(C + \lambda)}$$

In distributed fake traffic allocation algorithm, each sensor i in the iteration step k benefits from all other nodes current value x_i's, thanks to Flooding like algorithms, to update the value of $\mu^{(k)}$. Since all other nodes have access to such information too, they will obtain the same value for $\mu^{(k+1)}$ and therefore, we don't introduce additional notation to distinguish between the realized update processes. Upon updating $\mu^{(k)}$, each sensor i calculates its fake traffic $x_i^{(k)}$, accordingly. The above rule will proceed until reaching some predefined notions of convergence. This algorithm is listed as Algorithm 1.

Algorithm 1: Distributed Fake Traffic Allocation

Initialization
Initialize C $\forall i = 1 \ldots n$.
Main Loop
Do until $max_i \left| x_i^{(k+1)} - x_i^{(k)} \right| < \epsilon$

1. At each sensor node, update the dual variable as following:

$$\mu^{(k+1)} = \left[\mu^{(k)} + \gamma\left(\sum_{i=1}^{N} x_i^{(k)} - C\right)\right]^+$$

2. Update x_i according to the following equation:

$$x_i^{(k+1)} = (\lambda + C)2^{-(\log_2^{\xi} + \mu^{(k)})} - \lambda_i$$

4. Theoretical Analysis of Interval indistinguishability

As discussed in section 3, the source location can be exposed when an attacker can distinguish between real and fake intervals. In this section we give theoretical analysis of Interval indistinguishability in EI-based systems.

Let Vi be the random variable representing the time between the i^{th} and $1+1^{th}$transmissions. Let μ is the random variable representing the desired mean i.e., $E[V_i] = \mu$. Now we investigate two intervals, a fake interval and a real interval.

Fake interval (I_f):
The inter-transmission times are iid random variables in fake intervals. i.e., V_i's are iid's and $V_i = \mu$. Therefore, in any fake intervalI_f, for anyV_{i-1}, $V_i \in I_f$.

$$E[V_i \mid V_{i-1} < \mu] = \mu \quad (7)$$

Real interval (I_r):
The real interval has both fake and real transmissions. Let E_i be the random variable representing the real or fake event reported in the i^{th} transmission. Then E_i can hold the values of R and F, where R denotes a real event and F denotes a fake event.

In most general scenarios, the inter-arrival times of real events is varied, therefore assume that E_i take the values F and R with arbitrary probabilities.

To reduce delay in real event transmission, the time between the transmission of real event and its preceding fake one is shorter than the mean μ. To adjust the ensemble mean, the time between successive one its longer than the mean μ. That is, in the transmission of real intervalI_r, for V_{i-1}, $V_i \in I_r$

$$E[V_i \mid V_i < \mu, E_i = R] > \mu \quad (8)$$

And

$$E[V_i \mid V_i < \mu, E_i = F] = \mu \quad (9)$$

Using (8) and (9) equations we get,

$$E[V_i \mid V_i < \mu, E_i = R] * \Pr[E_i = R] + E[V_i \mid V_i < \mu, E_i = F] * \Pr \quad (10)$$

$$> \mu * \Pr[E_i = R] + \mu * \Pr[E_i = F] = \mu \quad (11)$$

An inter-transmission time is shorter than μ, then it is called as short inter-transmission time and an inter-transmission time is longer than μ, then it is called as long inter-transmission time. Then equation (11) implies that short inter-transmission times are mostly followed by long inter-transmission times during real intervals. Therefore an equation (7), (11) implies that short inter-transmission times followed by long inter-transmission times occurred in real intervals than the fake intervals. A short inter-transmission time followed by long inter-transmission time is called sort long pattern. Sort-long pattern is illustrated in Figure

5. Related Work

At first, the source um location privacy was laid by D.Chaum in [20]. Since then the source location privacy has been drawing increasing research attention in wireless sensor networks. Reed was introduced an idea to preserving location privacy through onion routing [21], and the ways to provide location privacy in location based systems such as Global Positioning Systems was discussed by Gruteser and Grunwald in [26].

A formal model was introduced by the Kamat and Ozturk [11], [12] that includes base-line routing techniques and routing with fake sources. The local attacker model was introduced and they demonstrated these techniques are not suitable for to provide source location privacy. To solve the problem they had proposed phantom routing technique. To reduce the chance an attacker can collect the location information Yong Xi [16] was proposed GROW (Greedy Random Walk). The GROW is a source and sink based random walk. In [17], Hoh and Gruteser was proposed a path confusion scheme is anonymity-preserving routing. A problem with existing approaches is that message latencies become larger and energy costs become higher as a result of introducing protections for the privacy of a source location.

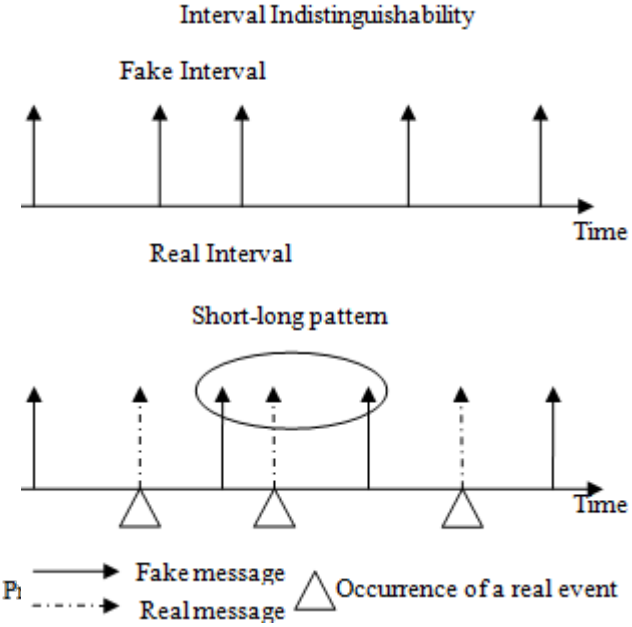

Figure 4: An illustration of short-long pattern

To overcome this problem a new cyclic entrapment method (CEM) [13] was proposed by Ouyang in [13]. In CEM local loops are introduced in the route at various points to trap the attacker and forcing to attacker to waste the extra resources.

In the global attacker model, the routing-based techniques are ineffective, because of global attacker have the entire view of a network; it can immediately detect the time and location of the event-triggered transmission. In [9], Mehta was introduced first global attacker model. In [9], two techniques were proposed that prevent the leakage of location information: periodic collection and source simulation. The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have

strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications.

One more method proposed for prevent the global adversary attacks: event source unobservability in [18] by Yang et al, which promises that a global adversary cannot know whether a real event has ever occurred even if he is capable of collecting and analyzing all the messages in the network at all the time. Clearly, event source unobservability is a desirable and critical security property for event monitoring applications, but unfortunately it is also very difficult and expensive to achieve for resource-constrained sensor network.

For the first time the notion of statistically strong source anonymity in [10], by Shao et al was proposed, under a challenging attack model where a global attacker is able to monitor the traffic in the entire network. For the notion of statistically strong source anonymity, a scheme was proposed called FitProbRate, which realizes statistically strong source anonymity for sensor networks. The goal in [10] is to minimize the latency of real events that are reporting while maintaining the statistical indistinguishability between fake and real events.

In [22], Shao et al also consider the security attacks on sensors with active adversary. For example, an attacker may attacks a node storing the event of his interest. To prevent this type of attacks they present pDCS, a privacy enhanced DCS network which offers data privacy on different security keys.

In recent works, to provide content confidentiality and source location privacy Li and Ren in [23] proposed a scheme which includes RRIN (routing to a randomly selected intermediate node) and NMR (Network mixing ring. RRIN provides local source location privacy and NMR provides global source location privacy. In [24], Ouyang et al four schemes were proposed: naïve, global, greedy and probabilistic to provide location privacy against global attacker. A distributed algorithm was proposed to mix real traffic with chosen dummy traffic to hide the real event traffic pattern in [25] by Abbasi et al. In [1], [2] B.Alomair et al were proposed a statistical frame work for source anonymity and also proposed binary hypothesis testing to remove or reduce the effect of noise information while transmitting data in sensor networks.

6. Conclusion and Future Work

In this paper, we provided a frame work for modeling source anonymity in sensor networks. We introduced the notion of interval indistinguishability to provide the source location privacy when the sensor networks launched in untrustworthy environments, and it avoids the source location information leakage. And we introduced distributed fake traffic allocation algorithm which establishes a fake traffic in entire network, when real event occurs it is embedding into the fake message.

Future work includes the mapping of source anonymity to coding theory in order to design efficient system that satisfies the notion of interval indistinguishability. And also to hide the source location from attackers establishes the dummy traffic in entire network and fake and real messages are embedded in to the dummy traffic. In addition, we are also interested in the implementation of our methods on real sensor platforms and the experimental results from real sensor applications.

References

[1] B. Alomair, A. Clark, J. Cuellar, R. Poovendran, "Toward a Statistical Framework for Source Anonymity in Sensor Networks," IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 248-260, 2013

[2] B. Alomair, A. Clark, J. Cuellar, R. Poovendran, “Statistical Framework for Source Anonymity in Sensor Networks,” in Proceedings of the 53rd IEEE Global Communications Conference–GLOBECOM’10. IEEE Communications Society, 2010.

[3] T. Arampatzis, J. Lygeros, and S. Manesis, “A survey of applications of wireless sensors and wireless sensor networks,” in Proceedings of the 13th IEEE Mediterranean Conference on Control and Automation – MED’05. IEEE Control System Society, 2006, pp. 719–724.

[4] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[5] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM Conference on Computer and Communications Security – CCS’02. ACM, 2002, pp. 41–47.

[6] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, “SPINS: Security protocols for sensor networks,” Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[7] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” in Cryptographic Hardware and Embedded Systems–CHES’06, ser. Lecture Notes in Computer Science, vol. 4249. Springer, 2006, pp. 46–59.

[8] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” in Cryptographic Hardware and Embedded Systems–CHES’07, vol. 4727, Lecture Notes in Computer Science. Springer, 2007, pp. 450–466.

[9] K. Mehta, D. Liu, and M. Wright, “Location Privacy in Sensor Networks against a Global Eavesdropper,” in Proceedings of the 15th IEEE International Conference on Network Protocols–ICNP’07. IEEE Computer Society, 2007, pp. 314–323.

[10] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards Statistically Strong Source Anonymity for Sensor Networks,” in Proceedings of the 27th Conference on Computer Communications INFOCOM’08. IEEE Communications Society, 2008, pp. 466–474.

[11] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source- Location Privacy in Sensor Network Routing," in Proceedings of the 25th IEEE International Conference on Distributed Computing Systems– ICDCS'05. IEEE Computer Society, 2005, pp. 599–608.
[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energyconstrained sensor network routing," in Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks–SASN'04. ACM, 2004, pp. 88–93.
[13] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, and U. Lowell, "Entrapping Adversaries for Source Protection in Sensor Networks," in Proceedings of the 7th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks–WOWMOM'06. IEEE Computer Society, 2006, pp. 32–41.
[14] X. Wang, X. Li, Z. Wan, and M. Gu, "CLEAR: A confidential and Lifetime-Aware Routing Protocol for wireless sensor network," in Proceedings of the 20th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications – PIMRC'09. IEEE Communications Society, 2009, pp. 2265–2269.
[15] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in Proceedings of the 29th Conference on Computer Communications – INFOCOM'10. IEEE Communications Society, 2010, pp. 1–9.
[16] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in Proceedings of the 20th IEEE International Parallel & Distributed Processing Symposium– IPDPS'06. IEEE Computer Society, 2006, pp. 1–8.
[17] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," in Proceedings of the 1st IEEE/CreatNet International Conference on Security and Privacy for Emerging Areas in Communications Networks–SecureComm'05. IEEE Communications Society, 2005, pp. 194–205.
[18] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in Proceedings of the first ACM conference on Wireless network security–WiSec'08. ACM, 2008, pp. 77–88.
[19] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," Elsevier Journal on Ad Hoc Networks, vol. 7, no. 8, pp. 1501–1514, 2009.
[20] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–90, 1981.
[21] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," IEEE Journal on Selected areas in Communications, vol. 16, no. 4, pp. 482–494, 1998.
[22] M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang, "pDCS: Security and privacy support for data-centric sensor networks," IEEE Transactions on Mobile Computing, vol. 8, no. 8, pp. 1023–1038, 2008.
[23] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks–SECON'09. IEEE Communications Society, 2009, pp. 493– 501.
[24] Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, "Source location privacy against laptop-class attacks in sensor networks," in Proceedings of the 4th international conference on Security and privacy in communication netowrks–SecureComm'08. ACM, 2008, pp. 1–10.
[25] A. Abbasi, A. Khonsari, and M. Talebi, "Source location anonymity for sensor networks," in Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference–CCNC'09. IEEE Communications Society, 2009, pp. 588–592.
[26] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in Proceedings of the 1st international conference on Mobile systems, applications and services–MobiSys'03. ACM, 2003, pp. 31–42.

Author Profile

Parthasaradhi M has done B.Tech from Sri Sai Institute of Technology and Sciences, Rayachoty, A.P. He is pursuing M.Tech from Gates Institute of Technology, Gooty, Anantapur, A.P., India.

B Nagalakshmi working as an Associate Professor, Department of CSE, Gates Institute of Technology, Gooty, Anantapur, A.P., India.

Prof D Venkatesh currently working as DEAN, CSE & IT departments of Gates Institute of Technology, Gooty, Anantapur, A.P., India. He has published 15 papers in various national and international journals. His areas of interest include MANETS, Data Structures, Computer Networks, Wireless Networks and Algorithms.