IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Preserving Source Location Privacy in Wireless Sensor Network

[1] Lilavati Samant , [2] Shrikanth N.G

[1]Computer Science & Engineering Department, VTU University,
SDIT, Mangalore, Karnataka. India

[2] Computer Science & Engineering, VTU University,
SDIT, Mangalore, Karnataka ,India

Abstract - The main aim of the paper is preserving location privacy by distracting attention from real data source. In this paper at random intervals the weights assigned to the link connecting the sensor nodes will be changed thereby following Shortest Path Algorithm in a random path. This attempt will achieve Source Location Privacy i.e. Anonymity. Data are kept secured with the help of Encryption Algorithm. Finally literature indicates how obscurity can be improved using the proposed model.

Keywords **- Wireless Sensor Networks (WSN), source location, privacy, anonymity, random path.**

1. Introduction

Wireless sensor networks have recently gained much attention as they can be readily deployed for different types of missions. In particular, they are useful for the mission that is difficult for human to carry out. For example, they are suitable for sensing dangerous natural phenomenon such as volcanic eruption, biohazard monitoring and forest fire detection. In addition to these hazardous applications, sensor networks can also be deployed for battle field surveillance, border monitoring, nuclear and chemical attack detection, intrusion detection, flood detection, weather forecasting, traffic surveillance and patient monitoring..

Monitoring networks consist of energy constrained nodes that are expected to operate over an extended period of time, making energy efficient monitoring an important feature for unattended networks. In such scenarios, nodes are designed to transmit information only when a relevant event is detected (i.e., event-triggered transmission). Consequently, the given the location of an event triggered node, the location of a real event reported by the node can be approximated within the node's sensing range.. There are three parameters that can be associated with an event to be detected and reported by a sensor node: the description of the event, the time of the event, and the location of the event. When sensor networks are deployed in untrustworthy environments, protecting the privacy of the three parameters that can be attributed to an event-triggered transmission and it becomes an important security feature in the design of wireless sensor networks. The security of transmitting a message can be achieved via encryption primitives. Hiding the timing and spatial Information of reported events cannot be achieved via cryptographic means. Encrypting a message before transmission, for instance, can hide the context of the message from unauthorized observers, but the mere existence of the cipher text is indicative of information transmission.

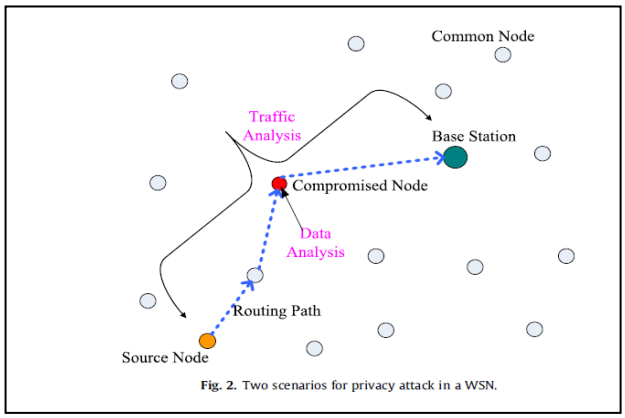

Fig. 2. Two scenarios for privacy attack in a WSN.

Fig1.[1] 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.

The source anonymity problem in wireless sensor networks is the problem of studying techniques that provide time and location privacy for events reported by sensor nodes. In this work, we present a scheme to hide source information using cryptographic techniques incurring lower overhead. The goal of the adversary is o identify the location and time of event of occurrence. To

hide the traffic pattern, randomly delaying the sending time is proposed to hide the parent-child relationship given a traffic rate model. Modelling the routing as a random process, the effectiveness of the random strategy depends on how randomness is introduced in the framework.

Performance of sensor nodes are evaluated in terms of four metrics: privacy,accuracy, delay time and power consumption. Features of WSNs such as Uncontrolled Environment, Sensor-Node Resource Constraints, and Topological Constraints puts unique challenges for privacy preservation in WSNs.

In general, the arrival distribution of random path is, in general, time-variant and unknown prior to it. To do that, nodes are required to transmit messages which comes from the source in Random manner, which can be achieved using Random Function which will generate random numbers in the range 0 to N(Number of nodes assumed to be present in the framework). The use of random walk is desired for protecting source location privacy. A random walk does not disclose any information about the source since the forwarding decision is made locally and independent of source location.

2. Model Assumption

In this Model, at random intervals weights assigned to sensor nodes will be changed. Let X is the time interval required to transmit message from 1 source to destination and X_R is the time interval when we are going to change weights assigned to the nodes. Then XR should be always greater than X. For example, if X=1sec i.e. time required to send message from Source to Destination then X_R should be approximately 15-20 minutes. This concept is used to reduce Power Consumption of battery charged Sensor Nodes.

In a Network where Destination will just receive the packets, Destination can handle more Computation Compare to the Source. Therefore while selecting an Encryption Algorithm, an algorithm should be such that it will impart less computation on encryption level i.e. at the source and accordingly complex decryption techniques should be selected.

3. Proposed Approach

Communication is assumed to take place in a network of energy constrained sensor nodes. Nodes are deployed to sense events of interest and report them with minimum delay. Consequently, given the location of a certain node, the location of the reported event of interest can be approximated within the node's communication range at the time of transmission. When a node senses an event, it places information about the event in a message and broadcast an encrypted version of the message. All sensor nodes will have their own private key and public key will be known to all the nodes in the network. In alteration to generating dummy packets we can transmit real events in multiple random paths towards the destination since it can not only cut down energy consumption but also it can minimize the communication overhead. Messages will be directed to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source. All the nodes will try to decrypt those messages. In this case only if the private key that is used for encryption is present with the receiving node the message can be decrypted to achieve the information. The more messages gets skipped from the adversary , the larger the safety period for the event and hence the source location privacy is provided. So even if adversaries are present on the path they cannot get the message and adversary may be led to the wrong source.

4. Performance Evaluation and Analysis

Delivery Time: Ideally the shortest delivery time is achieved if the packet is forwarded along the shortest path from the source to the sink To provide source location privacy in traditional random walk, it is necessary to relax the requirement for the delivery time. This is because the packets are always forwarded through the shortest path; it is easy for the eavesdropper to backtrack the path. In our Model since at X_R intervals weights of sensor nodes are going to change it is possible to continue with Shortest Path Concept, without breaching the Source Anonymity.
Random Walk: The use of random walk is desired for protecting source location privacy. A random walk does not disclose any information about the source since the forwarding decision is made locally and independent of source location.

5. Experimental Results

This work is about developing A statistical framework using Java & Mysql. Java Simulator is used for simulating Sensor nodes. Since java is platform independent this language is used instead of traditional NS2 simulator. Using AES encryption Algorithm, data are encrypted. Data will leave the source node and will follow the Random Path generated using random function in the range 0-N. File will be encrypted and will be sent in various paths which are possible using shortest path Algorithm towards destination. Since message will be

sent in various random paths simultaneously adversaries will get confused. They will try to get the message and if they are on wrong path they will fail in getting the message within a limited timeframe and message will reach destination successfully. Then adversary might try the other path leading to a wrong Source. Once message has been reached it will be useless decrypting it. Even if Adversaries are found to be on Random Path or if adversaries succeed in getting the random path they won't get the message since the code required decrypting it, is with the recipient only. Message Packet Flow is encrypted in the binary format such that correlations analysis will fail to distinguish between messages. Since the Messages are sent at the same time via different paths event is indistinguishable resulting in anonymity of the node from where the message is received.

6. Performance

Proposed Statistical Framework will help to manually delay the message by randomly changing the weights assigned to the link connecting Nodes. It can also be used from any location and on any platform. Source obscurity can be demonstrated successfully using this framework.

7. Conclusion

The Source Location privacy can be achieved using the given framework and random walk with shortest path Algorithm which is being implemented and is a completely new technique. This Statistical Framework can be improved further for a moving target using more efficient cryptographic techniques.

References

[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "On Source Anonymity in Wireless Sensor Networks," in Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks–DSN'10. IEEE Computer Society, 2010, (Fast Abstract)

[2] 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.

[3] 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. [4] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained 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.

[05] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained 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.

[06] 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.

[07] 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–

[08] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," in Proceedings of the 1st IEEE/ Crenate International Conference on Security and Privacy for Emerging Areas in Communications Networks–SecureComm'05.IEEE Communications Society, 2005, pp.194–205.

[09] 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.

[10] 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.

[11] 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.

[12] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984

[13] M. Stephens, "EDF statistics for goodness of fit and some comparisons," Journal of the American Statistical Association, vol. 69, no. 347, pp. 730–737, 1974. Science, 1989.

Lilavati Samant. Is a M.Tech Student of Computer Science & Engineering Department of SDIT, Mangalore. She graduated with BE (Honours') in Information Technology from Goa University, Goa. She is currently pursuing her Masters in Computer Science & engineering at SDIT (Shree Devi College of Engineering).Her research Areas are Computer Networks, Wireless Sensor Networks and Cryptography.

Mr.Shrikant is an Assistant Professor in the Department of Computer Science & Engineering, affiliated to VTU university, at SDIT(Shree Devi College of Engineering).His research areas are: Computer Network, Database