IJARES/July 2014/Volume-2/Issue-7/1244-1249 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

IMPROVING OF SECURITY CONCERNING BASE STATION IN SENSOR SYSTEMS

B.Geethanjali[1], SP.Chandrakanth[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

Privacy of location has been an energetic area of research in the modern years. Privacy of location in sensor networks moreover falls under common structure of location privacy. Provision of location privacy within a sensor network is demanding. It is extremely costly pertaining conventional anonymous communication methods for hiding communication among sensor nodes as well as sinks. The communication modes of sensors can make known an enormous deal of appropriate information, which can make known the location information of crucial components in a sensor network. Measures of Location privacy need to be developed to put off adversary from determining physical locations concerning source sensors as well as sinks. Prior effort in protecting the location of monitored objects required to augment the safety period that is the number of messages sends by means of the source earlier than the object is located by means of the attacker. A global eavesdropper can effortlessly overcome the prior efforts by means of locating the initial node initiating the communication by means of the base station. The periodic collection as well as methods of source simulation can be employed for providing privacy of source-location. The periodic collection process achieve most advantageous privacy however can only be functional to applications that gather data at a small rate and do not contain severe needs on data delivery latency.

Keywords: Sensor network, Location privacy, Anonymous communication, Adversary, Eavesdropper.

1. INTRODUCTION:

In recent times, several techniques of privacy-preserving routing have been expanded in support of sensor networks [4]. Most of them are designed to defend against an adversary only competent of eavesdropping on a restricted section of network at a time. An extremely motivated adversary can effortlessly eavesdrop on complete network and overcome these schemes. Privacy of location has been an energetic area of research in the modern years. In the services of location-based, a user might want to recover location-based information devoid of revealing his location. Privacy of location in sensor networks moreover falls under common structure of location privacy [10]. The adversary supervises wireless transmissions to assume locations concerning critical communications on the other hand there are a number of challenges exceptional to sensor networks. Sensor nodes are generally battery powered, that limits their practical duration. A sensor network is often considerably well-built than network in supported living applications [8]. Provision of location privacy within a sensor network is demanding. An adversary can effortlessly intercept network traffic due to use of broadcast medium in support of routing packets and can make use of information like packet transmission time as well as frequency to carry out traffic examination and assume locations of monitored objects as well as data sinks [1]. Sensors as shown in fig1 typically include restricted processing speed as well as energy supplies. It is extremely costly pertaining conventional anonymous communication methods for hiding communication among sensor nodes as well as sinks. Due to restricted energy duration of battery-powered sensor nodes, these techniques have to be energy resourceful [11]. As communication in sensor networks is much more costly than computation, we make use of communication cost to compute the energy utilization of protocols. Location privacy is extremely significant, in particular in hostile environments. Failure towards defending information can totally subvert projected purposes of sensor network applications [3]. Measures of Location privacy need to be developed to put off adversary from determining physical locations concerning source sensors as well as sinks. In homogeneous network representation, all sensors have approximately the similar computing

capability, power sources, as well as normal lifetimes and this is a general network construction for numerous applications at present and will likely carry on to be accepted moving forward [6] [14]. It provides moderately simple analysis in research and simple deployment as well as safeguarding in field. Though our research can be functional towards numerous sensor platforms, on the whole sensors run off battery power, particularly in kinds of potentially hostile settings.

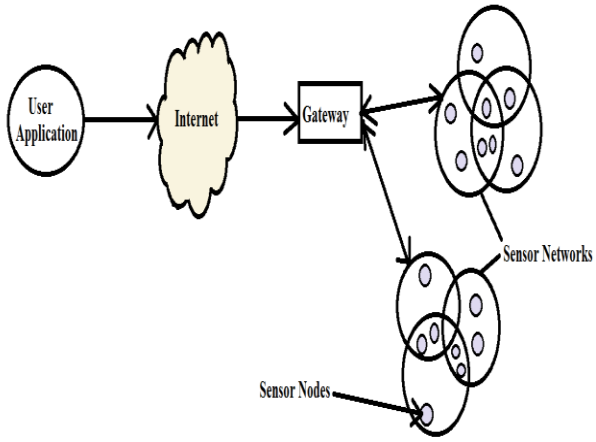

Fig 1: wireless sensor networks

2. METHODOLOGY:

The communication nodes of sensors can make known an enormous deal of appropriate information, which can make known the location information of crucial components in a sensor network. A technique to defend the sinks locations from a restricted eavesdropper by means of hashing the ID field within the packet header was introduced [9]. An adversary can follow sinks by means of functioning time correlation and attacks of rate monitoring. To alleviate these two kinds of attacks, a multiple-parent routing system, a scheme of random fake path, a hot spots and controlled random walk scheme, were introduced. Redundant hops and false packets are added to make available privacy when data are transmitted to the sink [7]. Prior effort in protecting the location of monitored objects required to augment the safety period that is the number of messages sends by means of the source earlier than the object is located by means of the attacker. The technique of flooding has the node of source send every packet all the way through numerous paths towards a sink, making it complicated for an adversary to mark out the source [2]. Fake packet generation generates false sources whenever a sender reports the sink that it has genuine data to send. The fake senders are away from the actual source and just about at the similar distance from the sink as the actual sender [13]. Phantom single-path routing attains location privacy by means of making each packet walk all along an

arbitrary path earlier than being delivered towards the sink. Cyclic entrapment generates looping paths at different places within the network to deceive the adversary into following these loops constantly and thus augment the safety period [16]. All these techniques take for granted a local eavesdropper who is only competent of eavesdropping on a minute region. A global eavesdropper can effortlessly overcome these schemes by means of locating the initial node initiating the communication by means of the base station. Methods such as k-anonymity in addition to private information retrieval have been developed for this intention. In persistent computing, users' location privacy can be negotiated by means of observing the wireless signals from the devices of user [12]. Phantom single-path routing attains location privacy by means of making each packet walk all along an arbitrary path earlier than being delivered towards the sink. The periodic collection process achieve most advantageous privacy however can only be functional to applications that gather data at a small rate and do not contain severe needs on data delivery latency [5]. The methods of periodic collection make available uppermost location privacy and are consequently constructive when we are monitoring extremely expensive objects. The source simulation means make available realistic trade-offs among confidentiality, communication transparency, as well as latency [15]. The sink simulation means accomplish location privacy through simulating sinks at particular locations, and backbone flooding means make available location privacy by means of flooding event reports in a backbone system that covers data sinks.

3. RESULTS:

The periodic collection as well as methods of source simulation can be employed for providing privacy of source-location. The methods of periodic collection make available uppermost location privacy and are consequently constructive when we are monitoring extremely expensive objects. The source simulation technique makes available a trade-off among confidentiality as well as communication costs. It is appropriate for scenarios where the object movement model can be accurately modelled and we require collecting instantaneous information from the network concerning the objects. The sink simulation as well as backbone flooding means can

make available location privacy in support of sinks. The backbone flooding means is obviously additionally appropriate for cases where a high level of location privacy is essential. The sink simulation means turns out to be more attractive, as it is additionally tough to node breakdown in network. In backbone flooding thought, we have to keep backbone associated and reconstruct backbone from time to time to stabilize communication costs among nodes.

4. CONCLUSION:

Most of privacy-preserving routing techniques are designed to defend against an adversary only competent of eavesdropping on a restricted section of network at a time. In the services of location-based, a user might want to recover location-based information devoid of revealing his location. As communication in sensor networks is much more costly than computation, we make use of communication cost to compute the energy utilization of protocols. In homogeneous network representation, all sensors have approximately the similar computing capability, power sources, as well as normal lifetimes. The sink simulation means accomplish location privacy through simulating sinks at particular locations, and backbone flooding means make available location privacy by means of flooding event reports in a backbone system that covers data sinks. An adversary can effortlessly intercept network traffic due to use of broadcast medium in support of routing packets and can make use of information like packet transmission time as well as frequency to carry out traffic examination and assume locations of monitored objects as well as data sinks. The source simulation technique makes available a trade-off among confidentiality as well as communication costs. The adversary supervises wireless transmissions to assume locations concerning critical communications. The source simulation means make available realistic trade-offs among confidentiality, communication transparency, as well as latency.

REFERENCES:

[1] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting Your Daily In-Home Activity Information from a Wireless Snooping Attack," Proc. Int'l Conf. Ubiquitous Computing (UbiComp '08), 2008.

[2] Protecting Location Privacy in Sensor Networks against a Global Eavesdropper Kiran Mehta, Donggang Liu, and Matthew Wright,2012

[3] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005.

[4] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.

[5] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '04), June 2004.

[6] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.

[7] V. Paruchuri, A. Duressi, M. Duressi, and L. Barolli, "Routing through Backbone Structures in Sensor Networks," Proc. 11th Int'l Conf. Parallel and Distributed Systems (ICPADS '05), 2005.

[8] H. Gupta, Z. Zhou, S. Das, and Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," IEEE/ACM Trans. Networking, vol. 14, no. 1, pp. 55-67, Feb. 2006.

[9] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.

[10] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008.

[11] T.S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno, "Devices that Tell on You: Privacy Trends in Consumer Ubiquitous Computing," Proc. USENIX Security Symp., 2007.

[12] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.

[13] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

[14] D. Son, A. Helmy, and B. Krishnamachari, "The Effect of Mobility Induced Location Errors on Geographic Routing in Mobile Ad Hoc Sensor Networks: Analysis and Improvement Using Mobility Prediction," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 233-245, July/Aug. 2004.

[15] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006

[16] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.