Providing An Efficient Way To Maintain Anonymity In Wireless Sensor Networks Based On Bogus Data

Hafez Rousta Sekehravani, Homayun Motamani, Babak Shirazi

Abstract: Wireless sensor networks can be used to supervise sensitive data or to monitor moving objects in a military environment. Anonymity in wireless sensor networks has become one of the major problems in the network since node localization data sender is crucial in these environments. However, lack of resources in wireless sensor networks present new challenges and create a network of anonymous. This paper attempts to provide a lightweight and efficient method to create anonymity for a wireless network and their nodes and compare and analyze the characteristics and advantages of the proposed method.

Index Terms: Anonymity, Bogus data, Security, Wireless sensor networks.

1 Introduction

Sensor network consists of large number of sensor nodes, which are widely spread in the environment to gather the data processing environment. Necessarily, the place of sensor nodes predetermined and it is unclear. This feature makes it possible to take them into dangerous or unavailable places [6]. One of the main applications of these sensor networks is to use them in defense industries and military environment. These sensors can be used to monitor forces, to control the military, to identify the opposing forces, to identify and detect the enemy chemical, biological and nuclear attacks [7]. But applying this technology in the military industry requires anonymity and the lack of identification of network nodes. Moreover, one of the main constraints in sensor networks nodes is the lack of energy resources. Sensors nodes usually have limited resources that cannot be non-reinforcement [8]. Therefore, the use of lightweight techniques and algorithms to maintain the anonymity are main concerns of the use of wireless sensor networks in the military. In this paper, we propose a method to increase privacy by the least amount of overhead load in the resource and network. This paper is organized as follows; part two reviews some of the studies that analyzed their strengths and weaknesses. In third section, we will evaluate the privacy of different models in the wireless sensor networks. Fourth part will be described the proposed approach based on the use of dummy packets and control packets. In Section five, the simulation software NS2 will be used to evaluate and discuss the proposed model and finally conclusion and future work will be described.

- *Master Student in Information Technology, Science and Technology University, Babol, Iran* h.roosta@ustmb.ac.ir
- *Department of Software Engineering, Islamic Azad University , Sari, Iran* motameni@iausari.ac.ir
- *Department of Information Technology, Science and Technology University ,Babol , Iran* b.shirazi@ustmb.ac.ir

2 Literatures Review

Detailed Research on anonymity in wireless sensor networks and similar areas such as private wireless networks, data extraction and location-based services are increasingly popular. Some experts carried out some studies in this field [1][2]. Mr. Shaw and et al[1] have proposed a model of the FPR. This modelis performed to deal with attacks from outside the network traffic by analysis of sensor networks and is considered to be perfectly symmetrical. In this model the end-to-end encryption technique is used. In fact, the intermediate nodes are not able to detect the transmitted packet is a packet data or a dummy package and no overhead. Mr. Yang and et al [3] have developed a model and have assigned a set of nodes in the model that have the ability to identify data and data overhead. In this way, they can reduce network overhead and energy that have been wasted. But the proposed model is still very heavy and expensive, since there is no difference in the length of the data packet and overhead. Also Mr. Chryand et al [4] propose a model, which to spread the base station receives data dissemination network to different intensities to make the enemy confused and disoriented. Furthermore, Mr. Ryndland et al [5] have tried to send the data by the base station to maintain anonymity even when no change has occurred in the nature of basic node. But both proposed model are listed as having too much overhead and cause energy waste in the long-term base station in the network and stop it.

3 Evaluations of different privacy models

• Send information as flood

In this method, an index is assumed as a benchmark to measure intended to protect the confidentiality of the node. When this indicator of a node pass through a certain limitation, all maintaining the confidentiality of nodes in the network send data that the enemy does not recognize the node position [10].

• Data transmitting and synthetic traffic

The basic idea of this method is hiding data within other dummy data that are sent along with the actual data. This method is created based on the chosen strategies that can send broadcast the actual data transmission through the existence nodes in the network bogus during the network [11].

• Use encryption

This method will try to take advantage of one-way hash functions and encryption techniques to encrypted data sent by

the nodes in such a way that the enemy or penetrating couldn't read the sent information and determine their position by nodes [12].

4 Proposed Solution

Wireless sensor networks are consisted of large number of sensor nodes. In order to maintain the confidentiality in these networks, the nodes without information send the dummy packets that may be associated with information nodes. If all sent data packets have equal length with the bracket[1], they impose high overhead on the network. In continue, we have tried to reduce the amount of overhead on the network and use the power grid more efficiently by using bracket controls. In the proposed project, a node can be placed in idle and ready state. In time, according to an exponential probability function, the node sends a control packet. The amount of this package controls indicate whether the node has information to transmit or not. The node that sends the control packet with F value means that it has no data for sent. However, The node that sends the control packet with a T value meanings that contain the information to be sent and will send them in the M match. In the M range, a node, which contains data information send dummy packages and other nodes.

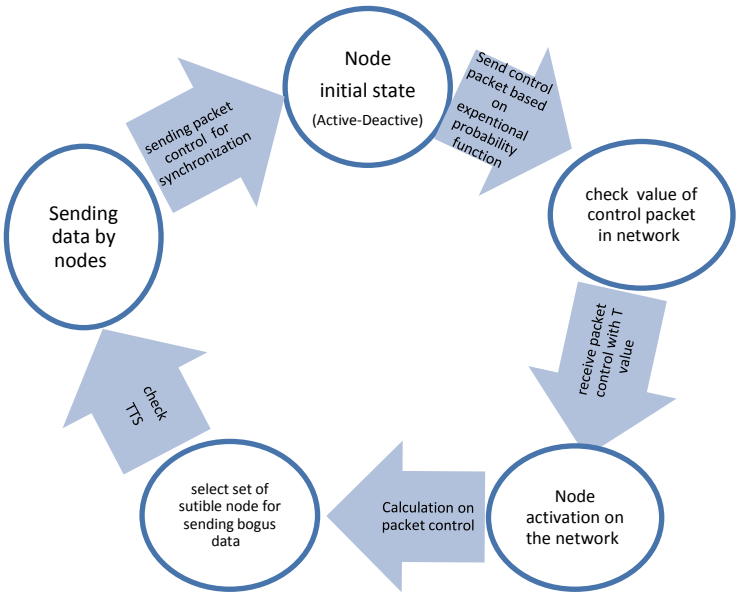
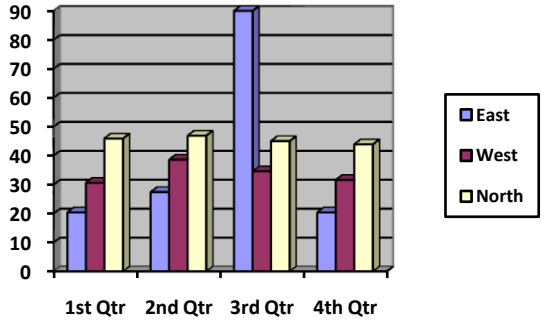


Figure 1: Overview of proposal approach



A node is ready when it has one of the following conditions:

- Has Information to be sent
- Received control packet with T value

If a nod has information to send, it will send T control information and this control message will be sent to all nodes in the network. Thus, all nodes in the network will be ready. Among active nodes, the nodes that meet the following criteria will be selected to transmit false information:

- Control packets have the maximum number to jump to reach them.
- Nodes with the highest, lowest and average M time interval

Consequently, in the specified period, the selected nodes will send real or fake data, and then will return to the idle position. The switched from active to idle mode, sending data back to idle mode can be considered as the cycle in the network to synchronized network by packet monitoring. In the proposed model, the length of the data packet length is more that manageable packets. In our model, we have considered the data packet length equal standard length of 30 bytes [9] and the application of sensor network packet control can be varied but here depending on the control we are considered packet control field as;

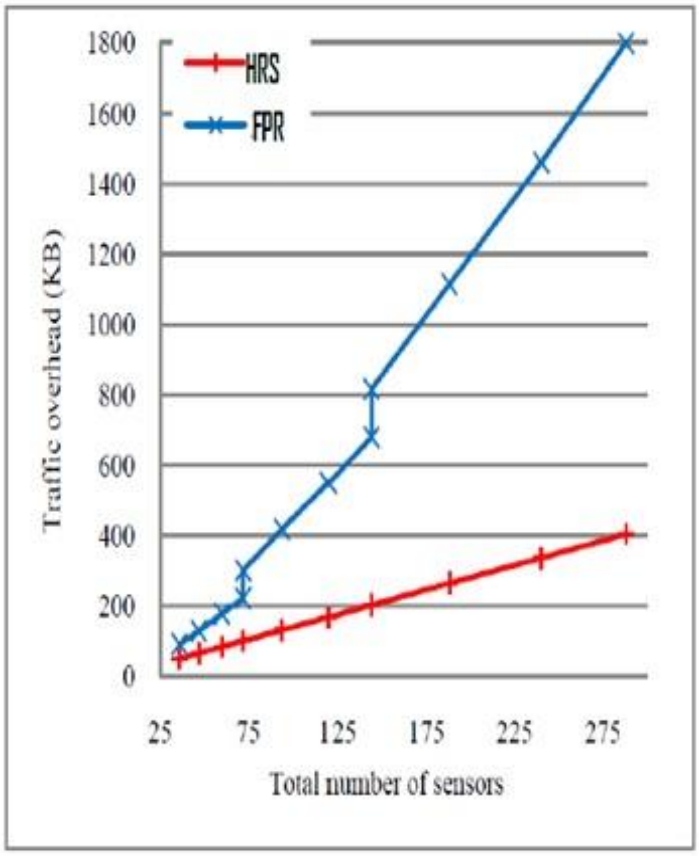
PH	$MI(ID_r, C_r, K_s, R)$	TTS

Figure 2: Structure of control packet

PH: it is an ID of the Specifies the control packet data, which is already transmitting control. The amount of this field has been considered equal to 15-bit that is sufficient for many wireless sensor networks to identify the nodes. This field helps received information nodes to broadcast received packet in network properly. MI: Contains additional information about the sender of a control packet. MI values were calculated by using one-way hash function and then are sent over the network. This field contains the number of control packet sender node identifier (ID r) and the number of times that the sender node has been ready to send data (C_r) and also contains a shared symmetric key (K_s) between the base station and the desired node. Thus, only the base station is able to detect the identity of transmitting node. The R value indicating whether the sender node contains data to be sent or not. TTS: This field contains 24 bits and specifies the expected time to send data. In fact, the purpose of this field is to synchronizing nodes for transmitting packets and real data. Accordingly, the maximum size of control packet length is 56 bits or 7 bytes.

5 Evaluating the Proposed Method using NS2 Software

In the computer software, NS2 is the network simulator, a discrete event simulator based on object oriented. This software was written by C programming languages and OTc1 and this is one of the most useful tools for simulating local and wide network area [13].



In order to evaluate proposed method, (HRS) have been compared with FPR in sseleriw networks by using NS2 software. The criterion of this comparison is the imposed overhead on the network against with increasing number of nodes in the network [13] In this simulation, we consider a fixed network size and consider the number of nodes for both the initial state equal to 25 nodes. Then, we have increased the nodes of the network to 275 nodes, and we have measured the amount of imposed overhead on the network. Based on the results of the simulation that are shown in Figure 3, the proposed method imposed the less overhead on the network in compare to the FPR. Additionally, this overhead is increased more and more remarkable by the number of nodes in the network, because the FPR method uses the huge packet to maintain the confidentiality over the network. Otherwise, in the proposed method, we have been used the control packet for maintaining the confidentiality of the packages and offered some ways to select nodes for sending bogus packages. Therefore, the overhead imposed on the network is done slowly by increasing number of nodes in the network.

6 Conclusion

In this paper we have presented a method to increase efficiently the privacy in sensor networks. One of the issues rose in the discussion of privacy is the overhead imposed on the network to get privacy. In the proposed method, based on the performed simulations, the synthetic traffic packets that are sent over the network was dramatically reduced by using appropriate nodes depending on the control and the adoption of dummy packets, so the network resources are used efficiently.

References

[1] M. Shao, Y. Yang, S. Zhu, and G. Cao," Toward s Statistically Strong Source Anonymity for Sensor Networks," in Proc. of the IEEE INFOCOM 2008, pp. 51-55, 20

[2] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurth,and T. La Porta, "Cross-Layer Enhanced Source Location Privacy in Sensor Networks," in Proc. of the IEEE SECON '09, pp. 1-9, 2009

[3] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G.Cao, "Towards Event Source Unobservability withMinimum Network Traffic in Sensor Networks," in Proc. of the ACM WiSec, Mar. 2008, pp. 77-88

[4] U. Acharya, M. Younis, Increasing base-station anonymity in wireless sensor networks, Ad Hoc Networks, Volume 8 Issue 8, November, 2010,Pages 791-809

[5] P. Rindl, Du. Xiaojiang, K. Nygard, “Light weight Source Anonymity in Wireless Sensor Networks ”,Global Telecommunications Conference (GLOBECOM 2011), 2011 IEE

[6] M. PejanovićĐurišić, Z. Tafa,G. Dimić, andV.Milutinović, A Survey of MilitaryApplicationsof Wireless Sensor Networks,MECO, Bar Montenegro, June 19, 2012

[7] Jun Zheng, Abbas Jamalipour, Wireless Sensor Networks: A Networking Perspective, John Wiley& Sons, England ,2009 ,page 229

[8] Michael Winkler, Michael Street, Klaus-DieterTuchs, KonradWrona, Wireless Sensor Networksfor Military Purposes, Autonomous SensorNetworks Springer Series on Chemical Sensors and Biosensors Volume 13, 2013, pp 365-39

[9] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensornetworks," in Proc. of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 162-175, 2004.

[10] CelalOzturk, Yanyong Zhang, and Wade Trappe. Source-location pri-vacy in energy-constrained sensor network routing. In SASN '04: Pro-ceedings of the 2nd ACM workshop on Security of ad hoc and sensornetworks, pages 88{93, New York, NY, USA, 2010

[11] Alomair, B., Clark, A. ; Cuellar, J. ; PoovendranR., Toward a Statistical Framework for Source Anonymity in Sensor Networks, Mobile Computing, IEEE Transactions on Volume:12 , Issue: 2 , Feb. 2013

[12] Joy Iong-Zong Chen, Chu-Hsing Lin, Algorithms for promoting anonymity of BS and for prolonging network lifetime of WSN, Peer-to-Peer Networking and Applications, January 2013

[13] Introduction to NS-2, Dr. Donald C. Wunsch II, Dr.Larry Pyeatt, Tae-hyung Kim, Department ofElectrical Computer Engineering University of Missouri-Rolla, USA,2006