International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol. 1, Issue 2, December 2014

Statistical Framework for Enhancing Source Location Privacy in Wireless Sensor Networks

Keerthi Neeluru
Intell engineering college

Abstract: **Wireless Sensor Networks (WSNs) became popular for many real world applications. The applications include monitoring wildlife habitat, surveillance, studying environments and a host of them in civilian and military context. Especially when WSN is used to have sensitive communications, security is an important concern. The security to messages can be achieved using various existing solutions found in the literature. However, the location of the sensor nodes from which data is collected is also to be secured. Thus source anonymity became a challenge problem in such networks. Unauthorized people can obtain information regarding location of the source of data by analyzing the messages being transferred. Therefore it is inevitable to protect messages and also ensure source anonymity. Recently Amomair et al. presented a framework for analyzing and evaluating source anonymity. This solution uses the notion of "interval indistinguishability" besides using a quantitative measure to achieve desired security in WSN. It also maps the problem to binary hypothesis testing so as to prove the efficiency of the solution. In this paper we implement a solution using NS2 simulations. The empirical results are encouraging.**

Index Terms – Wireless Sensor Network (WSN), security, source anonymity

I. INTRODUCTION

Wireless Sensor Networks (WSNs) became very useful in the real world. It can be said that they became ubiquitous with respect to usage in the areas of civilian and military applications for wide range of solutions. For instance they can be used in video surveillance, monitoring environment and studying wildlife habitat to mention few applications of WSN [1], [2], [3]. WSN is a collection of nodes that have limited resources. This is the main problem in them and they are vulnerable to various kinds of attacks. For this reason energy efficient methods are very important for WSN. One such method is event-triggered transmission which lets the sensor nodes to respond to only events so as to save energy for long lasting network. The general WSN is shown in Figure 1.

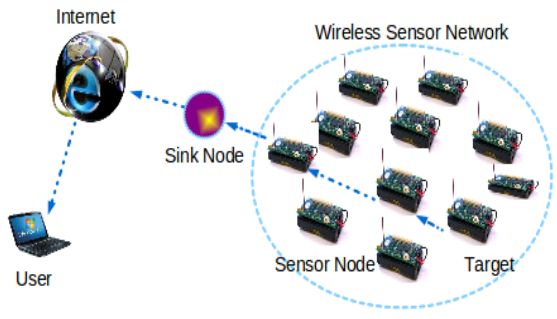

Fig. 1 – Typical wireless sensor network

As can be shown in Figure 1, wireless sensor network is a collection of sensor nodes which can sense data about targets. The sensor nodes sense the unknown object data and send to sink node. The sink node can be accessed by authorized users through Internet. In fact the sink node can be queried in order to monitor the area under coverage of WSN. Now let us take a real world scenario where sensors are deployed and there source anonymity plays a vital role in protecting data and location of sensors. Figure 2 shows one such network which is deployed in battlefield.

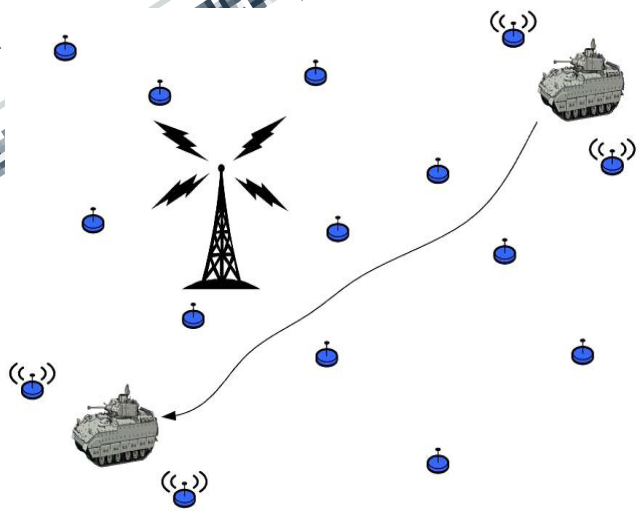

Figure 2 – Sensor network deployed in battlefield [15]

As can be seen in Figure 2 it is evident that every node deployed in battlefield can have its own sensing range and they can report events pertaining to combat vehicles which are targets for WSN. The movement of the combat vehicles is to be known by the sensor network. The parameters important include event description, time the event occurred and the place where event took place. Protecting the privacy of these three parameters play a pivotal role in securing communications in such WSN which is deployed in unsecure place and hostile environment. Previous research on such scenarios was explored in [1] and [2]. Using cryptography technique becomes costly in WSN. There has been research on the topic source anonymity in WSN as explored in [3]. There are many routing based solutions that assume local adversaries are explored.

In this paper we model a solution which is influenced by the solution in [4] and we implement an algorithm as described in section 3. Our solution is based on Simulations built using Java programming language. In fact we built a custom simulator (a prototype application) that demonstrates the proof of concept. The remainder of the paper is structured as follows. Section 2 reviews literature. Section 3 presents the proposed approach to solve source anonymity problem. Section 4 presents the experimental results while section 5 concludes the paper.

II. RELATED WORKS

There were many researches on the privacy problems pertaining to communications in WSN. The most recent research was from Alomair et al. [4] presented a novel framework that is capable of modeling and evaluating source anonymity in WSN. The other work which is close to the work of Alomair et al. made that contains similar model. Many solutions came into existence on sink anonymity in WSNs. The source anonymity is the problem pertaining to wider problem in WSN i.e., designing communication systems with privacy or anonymity. The first work towards it was done by Chaum before it became an important research area. Location anonymity and anonymity through onion router concepts came into existence towards solving source anonymity problem In WSN. These researchers used Global Positioning System (GPS) to test their solutions empirically. Many solutions assume eavesdroppers close to the sink. Another scheme they proposed was named "phantom flooding scheme". A scheme was introduced which lets adversary to waste his resources so as to discourage such attacks in future. Source location privacy was introduced in by making a routing solution that routes data from different paths. In the work done in [5] and [6] it is proved that routing based schemes are not sufficient to provide complete privacy pertaining to source anonymity. In [6] global adversary model was introduced. Many schemes result in performance degradation in terms of overhead and delay in communication. The delay problem was addressed in [5] by introducing the notion of statistically strong source anonymity besides the global adversary model which monitors traffic for finding source anonymity. Another scheme goodness of fit test was introduced to know fake events and data aggregation models were introduced in where filtering takes place by intermediate nodes to avoid fake messages. These schemes reduce the problem of high communication rate in WSN. Source location privacy and content confidentiality was explored in through routing approach using randomly selected intermediate node and other similar concepts. Four different schemes were proposed in namely probabilistic, greedy, global and naïve. A distributed approach was presented to usage of dummy traffic in order to hide the traffic pattern of real events in the WSN.

III. IMPLEMENTATION

The environment used for experiments is NS2.35 and Ubuntu 12.04 running in a PC with 2GB RAM and core 2 dual processor. The experiments are meant for demonstrating source anonymity in WSN. The simulation results are presented below that will show how sensor nodes collect data from surroundings and send data to base station. The simulations also show the source anonymity achieved.

Figure 1 - WSN with nodes and sink

As can be seen in Figure 1, it is evident that the typical WSN is created with sensor nodes and a base station or sink. From the simulation it can also be known that node 4 is ready to collect data from neighbor nodes and send it to base station.

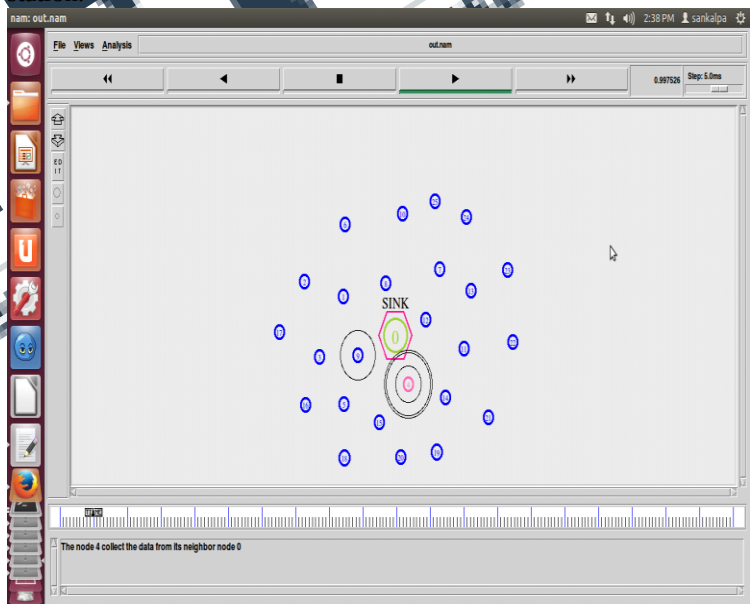

Figure 2 – Protocol propagation and nodes collecting data

As can be seen in Figure 2, the sensor nodes collect data from their neighbor nodes and also it showing the protocol propagation.

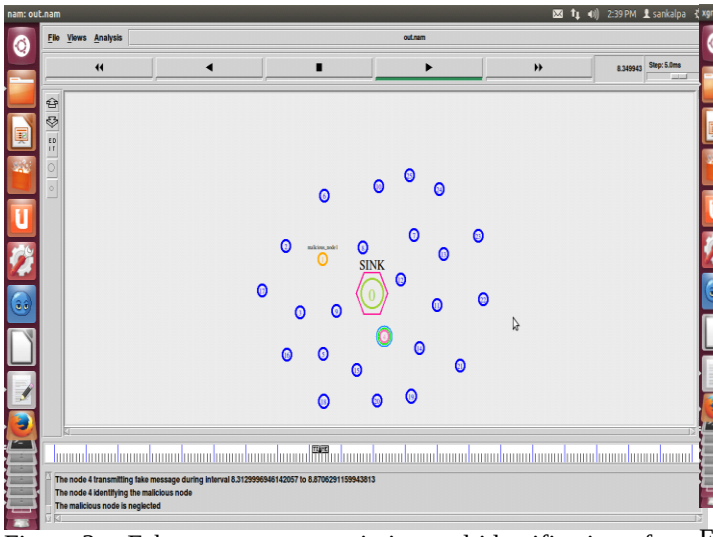

Figure 3 – Fake message transmission and identification of malicious nodes

As seen in Figure 3, it is evident that the fake messages employed in certain intervals can help in identifying nodes with malicious behavior.

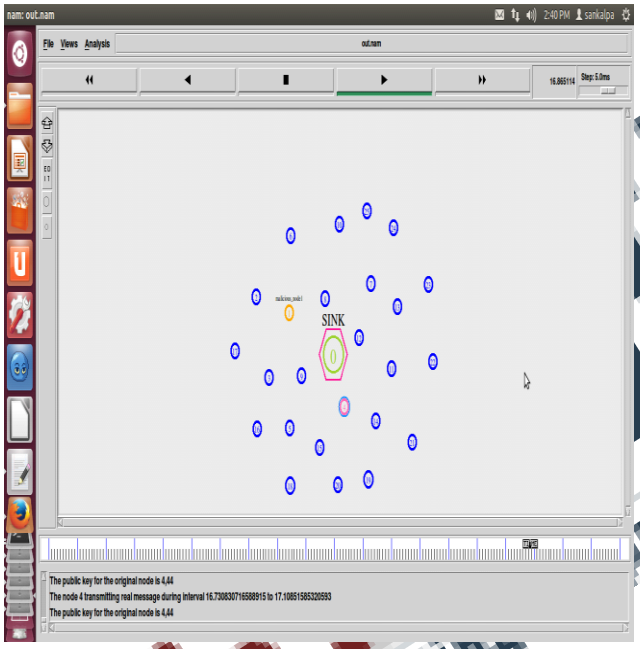

Figure 4 – Node gets public key and transmit real message

As can be viewed in Figure 4, it is evident that the sensor node gets public key for authentication and transmits real messages in specified time intervals. Moreover the source anonymity is achieved using the notion of "interval indistinguishability" besides using a quantitative measure to achieve desired security in WSN. It also maps the problem to binary hypothesis testing so as to prove the efficiency of the solution.

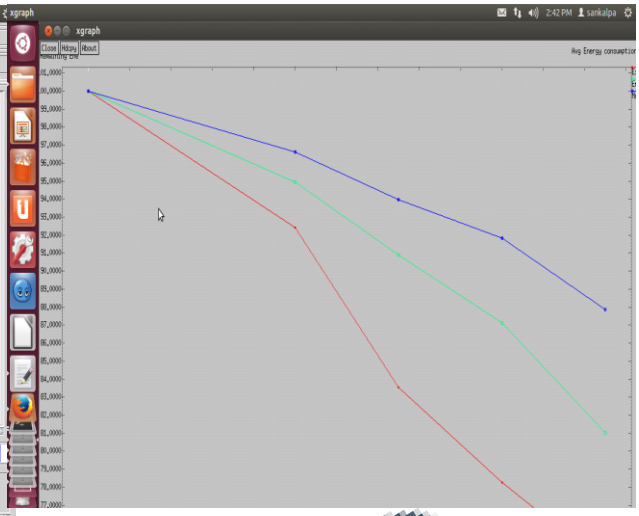

Figure 5 – Shows energy consumption graph

As shown in Figure 5, it is evident that the horizontal axis represents simulation time while the vertical axis represents energy consumption. As seen in graph it is known that as time passes there is significant decrease in energy consumption.

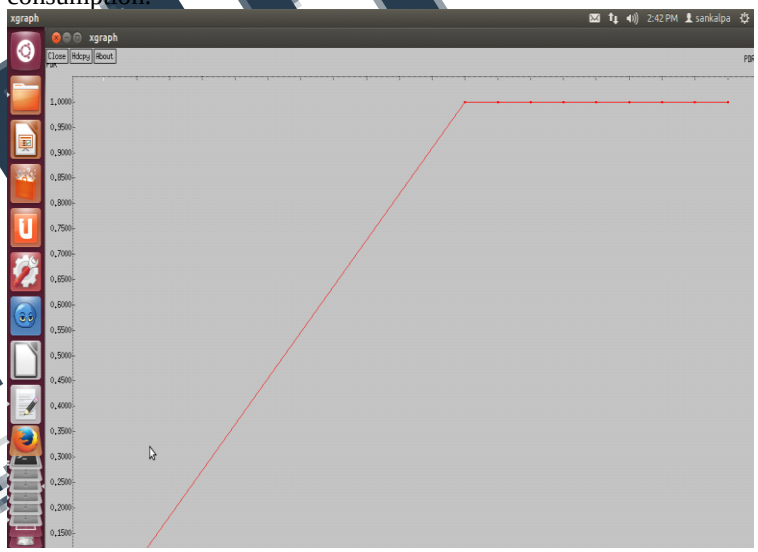

Figure 6 – Packet delivery ratio

As seen in Figure 6, it is evident that the horizontal axis represents simulation time while the vertical axis represents the time taken for packet delivery or in other words the packet delivery ratio. The experimental results reveal that the packet delivery ratio is increased as time passes.

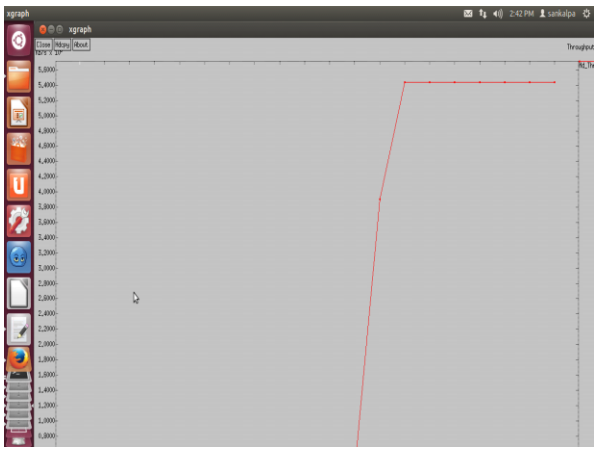

Figure 7 – Shows throughput dynamics

As shown in Figure 7 it is evident that the horizontal axis represents simulation time while the vertical axis represents the throughput values. The results reveal that throughput is increase as time goes on.

CONCLUSIONS AND FUTURE WORK

Wireless Sensor Networks (WSNs) became ubiquitous in the real world as they can be used in plethora of applications that encompasses both civilian and military fields. For instance they can be used in military operations and study wildlife habitat to mention few. Security is an important concern in such applications. Securing data being transmitted is not sufficient as the location of the nodes can provide clues to adversaries to guess unknown data. To avoid this source anonymity needs to be achieved. It is very challenging problem. Recently Alomair et al. presented a solution for source anonymity. In this paper we implement the notion of "interval indistinguishability" besides using a quantitative measure to achieve desired security in WSN. It also maps the problem to binary hypothesis testing so as to prove the efficiency of the solution. In this paper we implement a solution using NS2 simulations. The simulation results reveal that the solution is able to achieve source anonymity for fool proof communications in WSN. In future we continue research on source anonymity in other networks like MANET.

REFERENCES

[1] 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 Com- munications Society, 2008, pp. 466–474.

[2] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in Proceedings of the 15th IEEE Inter- national Conference on Network Protocols–ICNP'07. IEEE Computer Society, 2007, pp. 314–323

[3] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-layer Enhanced Source Location Privacy in Sensor Networks," in Proceedings of the 6th Annual IEEE communications society con- ference on Sensor, Mesh and Ad Hoc Communications and Networks–SECON'09. IEEE Communications Society, 2009, pp. 324–332

[4] Basel Alomair, Andrew Clark, Jorge Cuellary, and Radha Poovendran, Towards a Statistical Framework for Source Anonymity in Sensor Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.2 YEAR 2013, p1-13.

[5] 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.

[6] 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.