International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Protecting Source Location Privacy in Sensor Networks

Lintu Skaria[1], M.Ajin Milton[2]

PG Student,Department of CSE,Loyola Institute Of Technology And Science,Nagercoil,India[1]

Email: lintusthottathil@gmail.com[1]

Asisstant Professor, Department of CSE, Loyola Institute Of Technology And Science,Nagercoil,India [2],

Abstract- Wireless sensor networks are very useful nowadays because the modern networks are two way effective communication devices and also useful for monitoring the health of patient's, controlling the temperature of the machine in industries, battle field surveillance and so on. Advances in wireless sensor networks and location tracking methods are enabling location-based applications but they also form major privacy risks. Privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user's decision to release data. Though it is very useful in many ways, certain applications like location based reports are unidentified and unauthorized people can't detect such applications. This is one of the important privacy issues in the WSN. Many existing system proposed to address statistical resource anonymity tackle in the WSN. In previous work author proposed efficient framework to address the resource anonymity difficulty. In order to overcome the disadvantages in the existing system, like delay is more, lifetime of batteries is lower; overhead in the traffic and so on we introduce the efficient novel approach as coding theory. By using this approach, we address the problem of statistical resource anonymity in the wireless sensor networks. We carried out the some steps to address the anonymity trouble in the WSN. First we approach the idea of "interval indistinguishability" and this deal with the quantitative measure anonymity in WSN and then secondly, also produce the mapping for source anonymity problem by using binary hypothesis testing with respective parameters and dummy traffic are filtered using proxies.Our proposed method is efficient and effective when compared to the existing system through the experimental and simulation analysis.

Index Terms- Wireless sensor networks (WSN), source location, privacy, anonymity, hypothesis testing, nuisance parameters and Coding theory.

1. INTRODUCTION

Wireless sensor networks (WSNs) [2] are distributed collections of sensors with limited capabilities for computations and wireless communications. It is envisioned that WSNs will be used in a wide range of applications areas such as healthcare (e.g., patient monitoring), military operations (e.g., battlefield surveillance), and homes (e.g., home automation and monitoring).These WSNs will often be deployed in hostile environments where communications can be monitored, and nodes are subject to capture and surreptitious use by an adversary. Under such circumstances, cryptographic protection will be needed to ensure secure communications, and to support functions such as sensorcapture detection, key revocation, and sensor disabling. Unfortunately, many security schemes developed for general network environments do not take into account the unique features of WSNs: Public key cryptography is not feasible computationally because of the severe limitations imposed on the physical memory and power consumption of the individual sensors. To avoid resource anonymity is a difficult task in the wireless sensor networks that have inadequate resources in energy, working out and effective communication. Hence, only trivial, energy efficient privacy-preserving mechanisms are inexpensive. Therefore, it is also probable for an unauthorized observers to monitor all the total network traffic either by deploy his own sensors that cover up the whole operation area or by employing a controlling location surveillance gadget with inquiry range no less than the network radius. In spite of its consequence, so future, wireless sensor resource anonymity has not acknowledged sufficient concentration, and the existing approaches have restrictions when straight applied to wireless sensor networks. This is not only because the privacy problem is different but also because these techniques are too expensive to be employed. To get the address of statistical resource anonymity problems in the wireless sensor networks, the authors proposed many approaches but fails to address such anonymity problem in the WSN. The resource anonymity trouble in wireless sensor networks is the difficult of studying methods that some related to the time and location privacy for events reported through sensor nodes. In the previous work, the author proposed some framework to address the source anonymity problem in the WSN, in this

method the author used to transmit the fake messages in the WSN for to detect the resource anonymity difficult. In order to overcome the statistical resource anonymity difficulties in the wireless sensor networks, we proposed new novel efficient method. In this method we using coding theory technique to address such location and time based privacy issues in the wireless sensor networks. Our contribution in this paper as follows:

- In this paper, we proposed the new effective idea in "time indistinguishability" to address the statistical resource anonymity issues in the wireless sensor networks.
- We also implement the mapping for the statistical resource problem in the wireless sensor networks by using some concept in the "time indistinguishability" with annoyance related parameters.
- Proxies are used to filter the dummy traffic
- Our proposed method is efficient and effective when compared to the previously existing approaches through simulation and experimental result analysis.

2. RELATED WORK

In this section, we will see the some of the related works to the intrusion detection system using different approaches:

Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald [1], Advances in sensor networking and location tracking technology enable location-based applications but they also create significant privacy risks. Privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user's decision to release data. However, privacy policies require user interaction and offer little protection from malicious service providers. This paper addresses privacy through a distributed anonymity algorithm that is applied in a sensor network, before service providers gain access to the data. These mechanisms can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. Osman Yağan, Member, IEEE, and Armand M. Makowski, Fellow, IEEE [2], We investigate the secure connectivity of wireless sensor networks under the random pairwise key predistribution scheme of Chan, Perrig, and Song. Unlike recent work carried out under the assumption offull visibility, here we assume a (simplified) communication model where unreliable wireless links are represented as independent on/off channels. We present conditions on how to scale the model parameters so that the network 1) has no secure node that is isolated and 2) is securely connected, both with high probability, when the number of sensor nodes becomes large. The results are given in the form of zero-one laws, and exhibit significant differences with corresponding result in the fullvisibility case. Through simulations, these zero-one laws are shown to also hold under a more realistic communication model, namely the disk model.

Min Shao, Yi Yang, Sencun Zhu, Guohong Cao [3] For sensor networks deployed to monitor and report real events, event source anonymity is an attractive and critical security property, which unfortunately is also very difficult and expensive to achieve. This is not only because adversaries may attack against sensor source privacy through traffic analysis, but also because sensor networks are very limited in resources. As such, a practical tradeoff between security and performance is desirable. In this paper, for the first time we propose the notion of statistically strong source anonymity, under a challenging attack model where a global attacker is able to monitor the traffic in the entire network. We propose a scheme called FitProbRate, which realizes statistically strong source anonymity for sensor networks. We also demonstrate the robustness of our scheme under various statistical tests that might be employed by the attacker to detect real events. Our analysis and simulation results show that our scheme, besides providing source anonymity, can significantly reduce real event reporting latency compared to two baseline schemes .

Mauro Conti, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia,Luigi Vincenzo Mancini [4], The contributions of this paper are two-fold: first, we design a private data aggregation protocol that does not leak individual sensed values during the data aggregation process. In particular, neither the base station (BS) nor the other nodes are able to compromise the privacy of an individual node's sensed value. Second, the proposed protocol is robust to data-loss; if there is a node-failure or communication failure, the protocol is still able to compute the aggregate and to report to the base station the number of nodes that participated in the aggregation. To the best of our knowledge, our scheme is the first one that efficiently addresses the above issues all at once.

Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham [5], Much of the existing work on wireless sensor networks (WSNs) has focused on addressing the power and computational resource constraints of WSNs by the dsign of specific routing, MAC, and cross-layer protocols. Recently, there have

been heightened privacy concerns over the data collected by and transmitted through WSNs. The wireless transmission required by a WSN, and the self-organizing nature of its architecture, makes privacy protection for WSNs an especially challenging problem. This paper provides a state-of-the-art survey of privacy-preserving techniques for WSNs. In particular, we review two main categories of privacy-preserving techniques for protecting two types of private information, data-oriented and context-oriented privacy, respectively. We also discuss a number of important open challenges for future research. Our hope is that this paper sheds some light on a fruitful direction of future research for privacy preservation in WSNs.

Clark, A. Cuellar, J Poovendran, R [6], In this work, we investigate the security of anonymous wireless sensor networks. To lay down the foundations of a formal framework, we develop a new model for analyzing and evaluating anonymity in sensor networks. The novelty of the proposed model is twofold: first, it introduces the notion of ``interval indistinguishability'' that is stronger than existing notions; second, it provides a quantitative measure to evaluate anonymity in sensor networks. The significance of the proposed model is that it captures a source of information leakage that cannot be captured using existing models. By analyzing current anonymous designs under the proposed model, we expose the source of information leakage that is undetectable by existing models and quantify the anonymity of current designs. Finally, we show how the proposed model can lead to a general and intuitive direction for improving the anonymity of current designs.

. Di Ma ; Tsudik, G [7], Wireless communication is continuing to make inroads into many facets of society and is gradually becoming more and more ubiquitous. While in the past wireless communication (as well as mobility) was largely limited to the first and last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, and even opportunistically connected operation. The purpose of this article is to examine security and privacy issues in some new and emerging types of wireless networks, and attempt to identify directions for future research.

Jiri Kiur [8], While a wireless sensor network is deployed to monitor certain events and pinpoint their locations, the location information is intended only for legitimate users. However, an eavesdropper can monitor the traffic and deduce the approximate location of monitored objects in certain situations. We first describe a successful attack against the flooding-based phantom routing, proposed in the seminal work by Celal Ozturk, Yanyong Zhang, and Wade Trappe. Then, we propose GROW (Greedy Random Walk), a two-way random walk, i.e., from both source and sink, to reduce the chance an eavesdropper can collect the location information. We improve the delivery rate by using local broadcasting and greedy forwarding. Privacy protection is verified under a backtracking attack model. The message delivery time is a little longer than that of the broadcasting-based approach, but it is still acceptable if we consider the enhanced privacy preserving capability of this new approach. At the same time, the energy consumption is less than half the energy consumption of flooding-base phantom routing, which is preferred in a low duty cycle, environmental monitoring sensor network.

3. PROPOSED WORK

In order to overcome the statistical resource anonymity difficulties in the wireless sensor networks, we proposed new novel efficient method. In this method we using coding theory technique to address such location and time based privacy issues in the wireless sensor networks. Our contribution in this paper as follows: In this paper, we proposed the new effective idea in “time indistinguishability” to address the statistical resource anonymity issues in the wireless sensor networks. We also implement the mapping for the statistical resource problem in the wireless sensor networks by using some concept in the “time indistinguishability” with annoyance related parameters. Our proposed method is efficient and effective when compared to the previously existing approaches through simulation and experimental result analysis. The proxy decrypts the message so that the proxy can differentiate real event messages from bogus ones. Second, the proxy drops the message immediately if it is a bogus message

3.1 . *Interval indistinguishability*

The adversary’s ability to distinguish between the real and fake event by means of statistical analysis. That is ,given a series of transmission of a certain node ,the adversary must be unable to distinguish with significant confidence ,which transmission carries real information and which carries fake transmission .IF denotes a time interval without any real event transmission and IR denotes a time interval with real event transmission.The two time intervals are said to be statistically indistinguishable if the distributions of intertransmission times during these two intervals cannot be distinguished with significant confidence.

3.2. *Event indistinguishability*

Event indistinguishability refers that the adversary’s inability to distinguish between real and fake event with significant confidence.For example, consider a sensor network deployed in an animal hunting. For certain time interval the hunter cannot find any animal

and there was no activity. Therefore, the sensor nodes has been transmit fake message during that interval

3.3. *Converting Real Valued Samples To Binary Code*

Every intertransmission time that is shorter than the mean value can be represented by the binary digit zero.Every intertransmission time that is longer than the mean value can be represented by binary digit one.

3.4. *Binary Hypothesis Testing*

In binary hypothesis testing ,given two hypothesis H0 and H1 and a data sample that belongs to one of the two hypothesis . The goal is to decide to which hypothesis the data sample belongs . That is the goal is to decide whether the interval consist of fake transmission only or contains real transmission.

time. Otherwise the adversary easily identify the time interval and backtrace to the source location easily.

encrypted real event messages into its message buffer. After a constant time, a message, either bogus or real, will be sent out from the proxy node.

3.6. *Real Event*

Whenever real event occur algorithm AR will be implemented. In the absence of real events,nodes are programmed to transmit dummy messages in place of real events. When real event happens,we will transmit real event as soon as possible in the next scheduled dummy message.

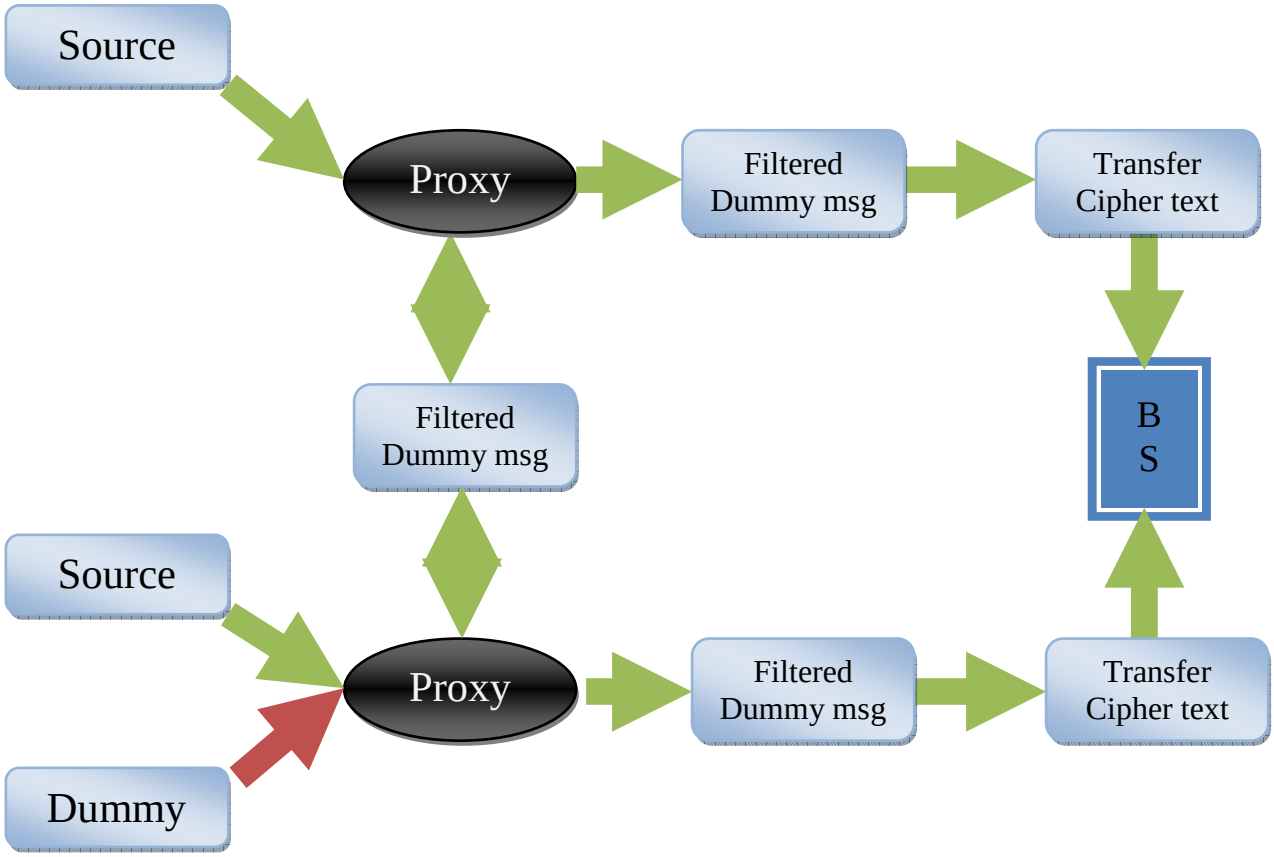

Fig. 1. Proxy filtering dummy message.

3.5. *Proxy Based Filtering Scheme*

First, the proxy decrypts the message so that the proxy can differentiate real event messages from bogus ones. Second, the proxy drops the message immediately if it is a bogus message. If on the other hand the message corresponds to a real event, the proxy re-encrypts the decrypted message. Third, the proxy puts this re-

4. CONCLUSION

Our proposed techniques in this paper, address the statistical resource anonymity difficulties in the wireless sensor networks by using the efficient coding theory. Our proposed coding theory is works

in the effective in the privacy preserving in the location and time based related reported sensor nodes. Our technique mapping also carried out for the source anonymity difficult in the WSN. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with previous cases. our proposed technique is also applied for the securing purposes in the wireless sensor networks. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

References

[1] Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald 'Privacy-Aware Location Sensor Networks"

[2] Osman Yağan, Member, IEEE, and Armand M. Makowski, Fellow,IEEE "Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links"- ieee transactions on information theory, vol. 59, no. 3, march 2013

[3] Min Shao, Yi Yang, Sencun Zhu, Guohong Cao "Towards Statistically Strong Source Anonymity for Sensor Networks"- This paper was originally published in the Proceedings of HotOS IX: The 9th Workshop on Hot

[4] Mauro Conti, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia,Luigi Vincenzo Mancini "Privacy-preserving robust data aggregation in wireless sensor networks" Article first published online: 14 JAN 2009

[5] Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham "Privacy preservation in wireless sensor networks: A state-of-the-art survey"

[6] Clark, A. Cuellar, J Poovendran, R "Statistical Framework for Source Anonymity in Sensor Networks"

[7] Di Ma ; Tsudik, G "Security and privacy in emerging wireless networks"

[8] Jiri Kiur "Privacy preserving protocols for wireless sensor networks"-

[9] H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks,"Elsevier J. Computer Networks,vol. 53, no. 9, pp. 1512- 1529, 2009.

[10] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-Layer Enhanced Source Location Privacy in Sensor Networks," Proc. IEEE Comm. Soc. Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), pp. 324-332, 2009.

[11] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query Privacy in Wireless Sensor Networks," ACM Trans. Sensor Networks,vol. 6, no. 2, pp. 1-34, 2010.