Maintaining Source Anonymity in Wireless Sensor Networks

Divya Luthra, Ruchi Anand, Shreeja Kumar, Rajeswari P

***Abstract*- The locations of events monitored by a sensor network often need to remain anonymous so that unauthorized observers are unable to detect the origin of such events by analyzing the network traffic. This is known as the source anonymity problem, which plays an integral role in the security of wireless sensor networks. To address this issue numerous techniques based on different adversarial assumptions have been proposed. In this paper, we propose a structure for modeling and analyzing anonymity in sensor networks. The novelty of this system is twofold: first, it introduces a concept through which source location tracking through wireless sensor network can be evaded; second, it incorporates hash-based message authentication code to safeguard the network traffic. What we establish is a global adversarial model, wherein undesirable performance characteristics, in the form of either relatively high delay or relatively high communication and computational overhead, are dealt with.**

***Index Terms*- Anonymity, security, source location, wireless sensor networks (WSN)**

I. INTRODUCTION

In many applications, such as military, animal tracking and health care, monitoring networks consist of energy constrained nodes that are expected to operate over an extended period of time; hence energy efficient monitoring becomes an important feature for sensor networks. To accommodate this, nodes are designed to be event-triggered, that is they transmit information only when a relevant event occurs.

There are three parameters that can be associated with an event detected and reported by a sensor node: the description of the event, the location of the event, and the time of the event. When sensor networks are deployed in unreliable environments, protecting the privacy of these three parameters becomes an important security feature in the design of wireless sensor networks.

While privacy in transmitting the "description" of a sensed event can be achieved through encryption methods, hiding the timing and spatial information of reported events cannot be achieved via cryptographic means. In simpler terms, the context of the message can be hidden by cryptography but the mere existence of a cipher text is suggestive of information transmission.

In the existing systems, the source anonymity problem has been discussed on two different scales, namely local and global adversarial models. A local adversary is one having limited mobility and partial view of the network traffic. Routing based techniques have shown to be effective in dealing with local adversaries. A global adversary has the ability to monitor the traffic of the entire network. Against global adversaries, routing based schemes are known to be ineffective. This is due to the fact that, since a global adversary has full spatial view of the network, it can straightaway detect the origin and time of the event-triggered transmission.

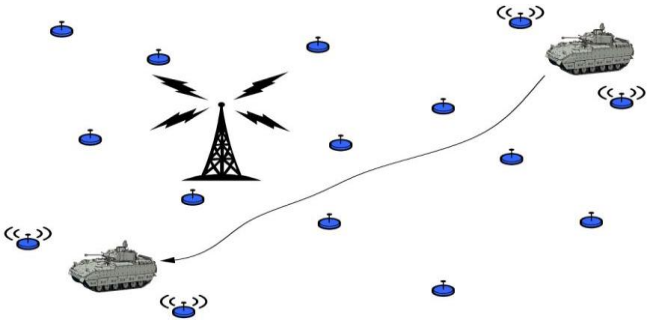

Fig. 1. A wireless sensor network in a battlefield. Nodes near the military vehicle broadcast information, while other nodes do not.

The primary step towards evading source tracking for sensor networks in the presence of global adversaries is to avoid event-triggered transmissions. In order to do so, nodes are programmed to transmit fake messages even if there is no detection of a real event. When a real event occurs, its information can be mixed with the transmissions of fake messages. Thereby for an individual transmission, an observer cannot conclude whether it is fake or real with a probability significantly higher than 1/2, assuming messages are encrypted.

In the above approach, there is an implicit adoption of probabilistic distribution to schedule the transmission of fake messages. If nodes report real events as soon as they are detected given the knowledge of the fake transmission distribution, statistical analysis can be used to identify real transmissions with a probability higher than 1/2, as illustrated in Fig. 2b. In other words, transmitting real information as soon as they are detected does not provide source anonymity against statistical adversaries analyzing a series of fake and real transmissions. This is known as the statistical source anonymity problem.

Manuscript received May 09, 2014

Divya Luthra, Telecommunication, Dayananda Sagar College of Engineering, Bangalore, India, 9538527565.

Ruchi Anand, Telecommunication, Dayananda Sagar College of Engineering, Bangalore,India, 8861062218.

Shreeja Kumar, Telecommunication, Dayananda Sagar College of Engineering, Bangalore, India, 9611018648.

Rajeswari P, Telecommunication, Dayananda Sagar College of Engineering,Bangalore,India, 9986013606

A way to alleviate the above statistical analysis is illustrated in Fig. 2c. Instead of transmitting the next scheduled fake event, the current real event details can be sent over the network. This introduces additional delay. However, addressing this problem by adopting a more frequent scheduling algorithm is impractical since sensor nodes are battery powered and many a times unchargeable. Therefore, a frequent transmission scheduling will drastically reduce the desired lifetime of the sensor network along with considerably increasing the communication and computational delay.

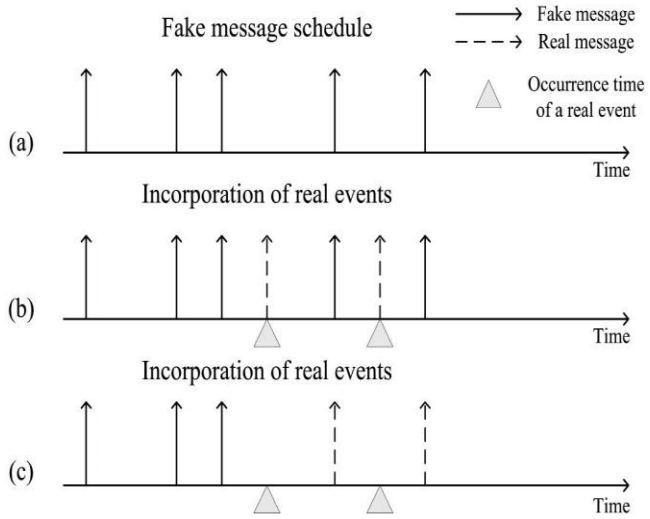

Fig. 2. Different approaches for embedding the report of real events within a series of fake transmissions, (a) shows the prespecified distribution of fake transmissions, (b) illustrates how real events are transmitted as soon as they are detected, (c) illustrates how nodes report real events instead of the next scheduled fake message.

The Statistical Source Anonymity (SSA) problem in sensor networks is the study of techniques that maintain source anonymity despite of global adversaries performing statistical analysis on node transmissions. Practical SSA solutions need to be designed to achieve their objective under two main constraints: minimizing delay and maximizing the life span of sensors' batteries.

II. RELATED WORKS

The foundation for source location privacy in sensor networks was laid by David Chaum in [1]. Topics related to location anonymity have been discussed by Reed et al. in [2] who introduced the idea of preserving anonymity through onion routing. Gruteser and Grunwald in [3] also discussed ways to provide anonymity in location-based services, such as Global Positioning Systems. In [4], Wang et al. proposed a technique to maximize source location privacy by designing routing protocols that distribute message flows to different routes. In the global adversarial model, proposed by Mehta et al. in [5] mentioned that the adversary has access to all transmissions in the network, routing based schemes are insufficient to provide location privacy. The authors to mitigate this problem, proposed two new schemes. In the first scheme, some sensor nodes act as fake sources by mimicking the behavior of real events. In the second scheme, packets (real and fake) are sent either at constant intervals or according to a predetermined probabilistic schedule. Although this scheme provides perfect location privacy, it also introduces undesirable performance characteristics, in the form of either relatively high delay or relatively high communication and computational overhead. To reduce the amount of traffic in the network that is due to the transmission of fake events, techniques based on node proxies and data aggregation have been proposed by Yang et al. in [6]. In such techniques, the overall communication overhead is reduced by making intermediate nodes act as proxies that filter out fake messages or by aggregating multiple messages in a single transmission. In recent works, Li and Ren in [7] proposed a scheme to provide both content confidentiality and source-location privacy through routing to a randomly selected intermediate node (RRIN) and a network mixing ring (NMR), where the RRIN provides local source location privacy and NMR yields network-level (global) source location privacy. Ouyang et al. in [8] proposed four schemes: naive, global, greedy, and probabilistic to protect the source location against global adversaries.

III. MODEL ASSUMPTIONS

The network and adversarial assumption that will be used in this paper are as follows.

A. Network Model

Communication is required to take place in an energy constrained sensor node network. Nodes are used to sense events of interest and report them with minimum delay. Subsequently, 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 broadcasts an encrypted version of the message. To hide the report of an event of interest, nodes are made to broadcast fake messages, even in absence of an event. Nodes are equipped with schemes to enable hash based message authentication code in order to secure the network traffic.

B. Adversarial Model

The adversarial model used in this system is a global one, such as shown in Fig.3. An external adversary is an adversary who has no control over the nodes in the network. Whereas active adversaries are those who inject their own traffic or jam the network, a passive adversary is only capable of observing the network traffic. A global adversary is an adversary who can monitor the traffic of the entire network and can determine the node responsible for the initial transmission reporting an event of interest.

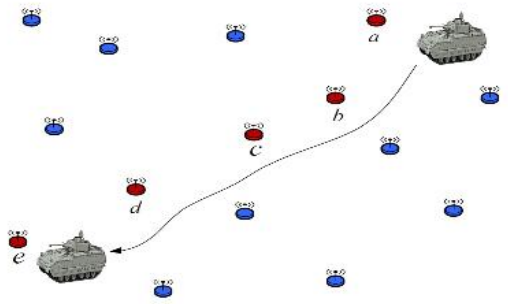

Fig. 3. An example of a sensor networks monitoring a moving target. As the tank moves along its path, nodes a, b, c, d, and e report that the tank is within their sensing range.

IV. SYSTEM DESCRIPTION

In this system we investigate the problem of source anonymity and design a system comprising of modules which evades source location tracking by a global adversary who is monitoring the network traffic.

A. Sensor Setting and tanker route configuration

We propose a quantitative measure to evaluate statistical data of the sensor network nodes and the tank position as shown in Fg.3. This is an initialization module which configures the sensor details and tank movement path details. Each sensor has its own identity and X & Y co-ordinates. With the help these parameters server can understand the location and identity of the sensor in close proximity with the tank.

B. Operation during real and fake events

We mitigate the problem of breaching source anonymity by using nuisance parameters which are fake events. The event of interest or the real event in question here is the exact location of the military tank. All the sensors monitor the area for the tank location. If the tank is in the vicinity of a sensor, it activates Algorithm AR, which is designed to carry out real information transmission in presence of a real event. These transmissions are embedded with fake information transmissions, controlled by Algorithm AF. When the tank starts to move, real and fake timer events are initiated. The real timer furnishes details of tank every 3 seconds to the sink. Message authentication code is generated for real information by making use of a hashing function. The fake timer monitors all the sensors except the one near to the tank. These sensors give fake details of tank every 6 seconds to the sink / server. These steps are illustrated in Fig. 4.This is the part of the system where the adversary can monitor the network traffic and hence is susceptible to eavesdropping. The simulation is shown in Fig. 7.

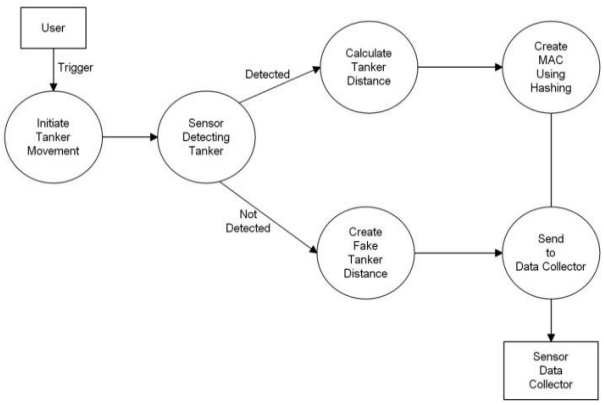

Fig. 4. Architecture of simulation system

C. Server Operations

The server operations are carried out by the supervisory entity. The admin who is the chief in command using the server has access to the server database which harbors all the data. The complete data, whether real or fake is visible to the admin.

D. Extract data and filter event details

This module fetches the sensor data from the database to server graphic user interface. In general all the sensor nodes details are showed in the server display grid. With the help of filter function, fake data are removed and the real data is filtered and showed to the admin as described in Fig.5. This provides the admin with a better understanding of the tank location. The extraction of original data by the filter function is done by using message authentication code to simultaneously verify both the data integrity and the authentication of the message as shown in Fig. 8.

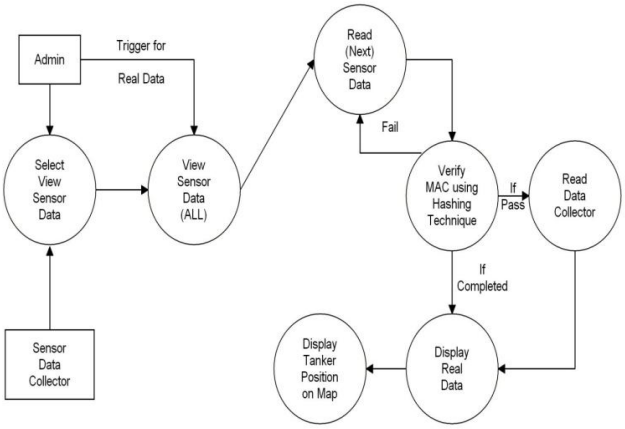

Fig. 5. Architecture of supervisory system

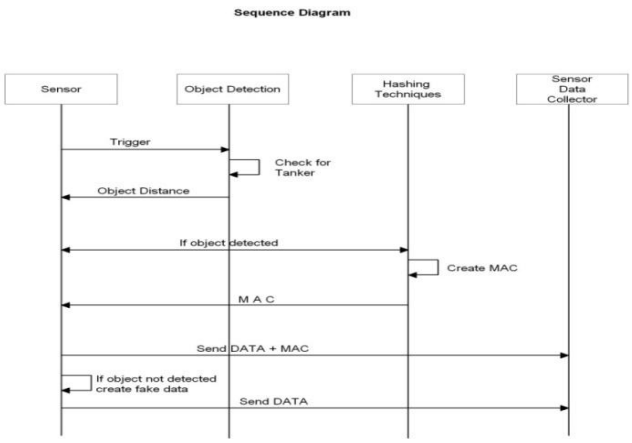

Fig. 6. Sequence diagram

V. CONCLUSION AND FUTURE SCOPE

In this paper, we provided a framework for modeling and analyzing source anonymity problem in wireless sensor networks. We introduced the notion of nuisance parameters in a predetermined probabilistic manner. We illustrated a way to prevent the adversary from modifying the network traffic by making use of hash based message authentication

code. Finally, we proposed a modification to existing routing solutions to improve the anonymity at a global network level.

Future extensions to this work would be mitigation of the problem of statistical source anonymity to design an efficient system that satisfies the notion of interval indistinguishability.

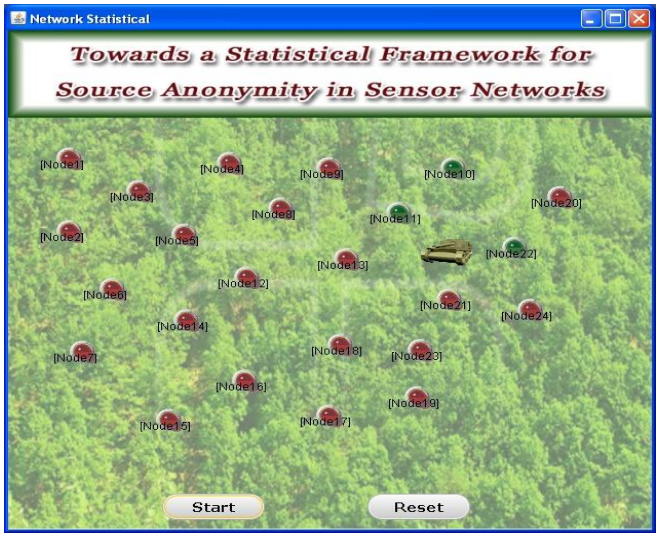

Fig. 7. Snapshot of simulation

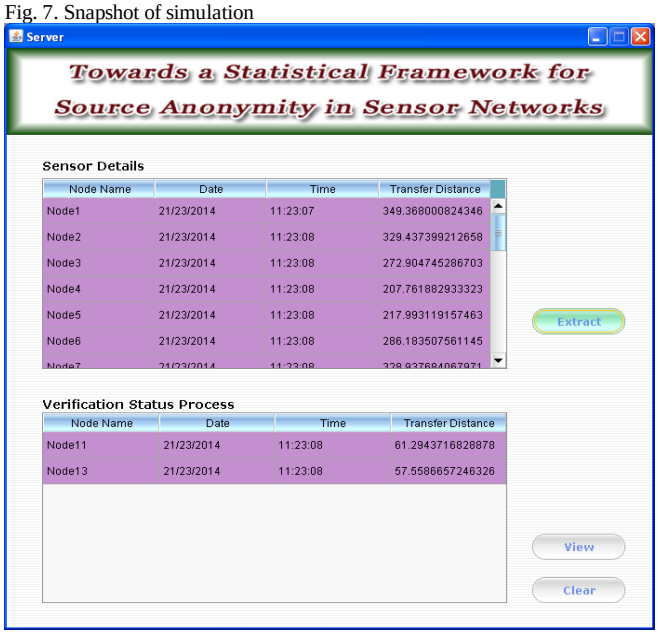

Fig. 8. Graphic user interface for supervisory system

REFERENCES

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84 90, 1981.

[2] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[3] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in *Proceedings of the 1st international conference on Mobile systems, applications and services–MobiSys'03*. ACM, 2003, pp. 31–42.

[4] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Elsevier Journal on Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.

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

[6] 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.

[7] 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.

Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, "Source location privacy against laptop-class attacks in sensor networks," in *Proceedings of the 4th international conference on Security and privacy in communication networks–SecureComm'08*. ACM, 2008, pp.1

Shreeja Kumar is currently an undergraduate, B.E student at Telecommunication Department in Dayananda Sagar College of Engineering, Bangalore. Her areas of interests are Wireless Sensor Network applications, its security and privacy, Wireless Communication and Digital Communication. She is currently working on a project entitled "Evasion of Source Location Tracking using wireless Sensor Networks" and has also published a paper in the 2nd National conference on Communication and Image Processing, 2014.

Ruchi Anand is currently an undergraduate, B.E student at Telecommunication Department in Dayananda Sagar College of Engineering, Bangalore. Her areas of interests are Wireless Sensor Networks and its applications, logic design, analog and digital communication. She is currently working on a project entitled "Evasion of Source Location Tracking using wireless Sensor Networks" and has also published a paper in the 2nd National conference on Communication and Image Processing, 2014.

Divya Luthra is currently an undergraduate, B. E student at Telecommunication Department in Dayananda Sagar College of Engineering, Bangalore. Her areas of interests are Network Security, Computer Communication Networks and Wireless Sensor Networks. She is currently working on a project entitled "Evasion of Source Location Tracking using wireless Sensor Networks" and has also published a paper in the 2nd National conference on Communication and Image Processing, 2014.

P. Rajeswari received her B.E Degree in Electronics and Instrumentation Engineering in 1997 from Government College of Technology, Coimbatore and the M.E. degree in VLSI Design in 2006 from Anna University. She is pursuing her PhD degree in SRM University, Chennai. She is currently working as an Associate Professor in the Department of Telecommunication Engineering at Dayananda Sagar College of Engineering, Bangalore. India.