Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Design and Development of Secured Wireless Sensor Network Environment with LSB Steganography

Rupali D. Shinganjude, Deepti P. Theng
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering
Nagpur, Maharashtra, India

Abstract— Sensor networks mainly deployed to monitor and report real events, and thus it is very difficult and expensive to achieve event source anonymity for it, as sensor networks are very limited in resources. Data obscurity i.e. the source anonymity problem implies that an unauthorized observer must be unable to detect the origin of events by analyzing the network traffic; this problem has emerged as an important topic in the security of wireless sensor networks. This work presents a framework that models the anonymity and adds better results to existing SAS model providing source anonymity by implementing source signature using LSB technique in sensor network. It introduces the interval and event indistinguishability and to evaluate anonymity it provides a quantitative measure and maps source anonymity with nuisance parameters. Performing so, we transform the analyzing real-valued sample points into study of anonymous sensor networks.

Keywords— Wireless sensor network, anonymity, statistical test, persistent dummy traffic, coding theory, steganography.

I. INTRODUCTION

Sensor networks have been envisioned to be very useful for a broad spectrum of emerging civil and military applications [2]. However, sensor networks are confronted with many security threats such as false data injection, disruption in routing and node compromise, as they normally operate in unattended, harsh or hostile environment. Among all these threats, privacy which is an important aspect of monitoring applications in wireless sensor networks (WSNs) has become a special interest since it cannot be fully addressed by traditional security mechanisms such as encryption and authentication. Sensor nodes in a sensor network when senses an event, it sends a message including event related information to the base station. If an attacker can intercept the message, the information of sensitive data can be gained. The networks consisting of energy constrained nodes, the nodes are expected to operate over an extended period of time, making energy efficient monitoring an important feature for networks that are still not attended. In such scenarios, nodes are designed to transmit information only when a relevant event is sensed (i.e., event-triggered transmission). There are three parameters that can be associated with an event detected and reported by a sensor node- the description of the event, the time of the event, and the location of the event [3]. The source anonymity problem in wireless sensor networks is the problem of studying techniques that provide time and location privacy for events reported by sensor nodes. The source anonymity problem has been drawing increasing research attention recently [1, 9].

As the sensor nodes deployed in the network are kept viewed by the opponent, the different features of opponent must be known before designing the anonymity model. Adversary (opponent) is categorized into external, passive and global [5]. External adversary will not compromise or control any sensors; passive attacker does not conduct active attacks such as traffic injection, channel jamming and denial of service attack; global adversary can monitor all the communications in the network and determine the node responsible for initialization of event transmission. Routing based techniques seems to be ineffective against global adversary which is effective against the local opponent. Therefore the research attention seems to increase in drawing source anonymity model against global adversary.

The step toward reporting real event without revealing their information to adversary is the idea of persistent dummy traffic. To refrain from event-triggered transmission nodes are made to transmit fake messages even if there is no detection of events of interest .When a real event occurs, its report is embedded within the transmissions of fake messages. Thus, the opponent cannot distinguish between fake or real events [3, 5, and 9]. The notion of interval and event indistinguishability is introduced here. If reports are introduced as soon as they are detected then statistical analysis can be used to identify outliers. Therefore opposing its transmission as soon they are detected they can be transmitted instead of next scheduled fake event.

II. PROPOSED SCHEME

The brief analysis on source anonymity in wireless sensor network results into the judgment that source anonymity is best achieved by using SAS model. As anonymity is measured by the amount of information about the time occurrence and location of reported events that an adversary can extract by monitoring the sensor network therefore Interval and Event indistinguishability in introduced.

A. Event Indistinguishability (EI)

Currently, as modelled the anonymity is measured by adversary's ability to distinguish between real and fake signal transmission. The main motto behind designing is that the adversary should not be able to distinguish between series with confidence that which information is real and which is fake one.

If an adversary continuously observing the network over multiple time intervals and during some instant of time if adversary is able to distinguish a change in behaviour of signal transmission then this change can work as an indication of real event existence, even though the adversary was unable to distinguish between individual transmissions. Here event indistinguishability means that one cannot distinguish between inter-transmission times between events reported by sensor nodes with significant confidence.

B. Interval Indistinguishability (II)

Source anonymity i.e. here source location privacy whose main motto is to hide the information about the occurrence of event of interest. This means that an adversary observing the sensor network traffic should not be able to distinguish between the intervals containing real event without worrying about the number of transmissions the adversary observes. Although giving too strong assumption if the adversary is able to notice a change statistical behaviour of transmission times of a certain node in the network then it indicates the existence of real activities.

Consequently, in many applications where nodes are tamper resistant and also not, all that is needed is to observe different time intervals. The more distinguishable a time interval from the known fake interval, the more likely it is to contain real events. To model interval indistinguishability, the game between challenger C and adversary A is proposed.

Game 1 (Anonymity game).

1. C chooses two intervals IR and IF, where IR is a real interval and IF is a fake one.
2. C draws a bit bϵ {0, 1} uniformly at random and sets IR=Ib and IF=Iɓ, where ɓ denotes the binary complement of b.
3. C gives Ib and Iɓ to A.
4. A makes any statistical test of her choice on Ib and Iɓ and outputs a bit b'.
5. If b' = b, A wins the game.

C. Nuisance Parameters

Nuisance parameters can be the noise or the unwanted parameters in the system which is here also being added in order to evaluate the system. The fake message transmission in the network which is not required but implemented to achieve new direction towards designing anonymity to source. In random traffic generating nuisance parameter is not much critical.

In designing anonymous sensor networks in the absence of real events, nodes are programmed to transmit independent identically distributed fake messages according to a certain distribution. In addition, the ProbRate scheme where message transmission rate follows a probabilistic distribution provides an opportunity for reducing latency, compared with the ConstRate scheme where message transmission rate is fixed. Hence, we prefer probabilistic message transmission intervals.

Algorithm 1: Random Traffic Generation
Input: mean value;
Output: a time interval following the random distribution with mean value;
Procedure RTG:
1: seed; (Assign seed as the seed for random number generation, a unique seed is preloaded in each sensor.)
2: return random (mean value);

Algorithm1 implements the idea of random distribution for dummy traffic generation. Suppose there are a series of dummy messages, our motto is to create the time intervals between two consecutive messages following random distribution with given mean value and global variable seed then the algorithm returns the time interval to transmit the next dummy message. A mean value is taken and the data transmission follows the time interval of mean value between each single signal. This generates a random traffic with mean value i.e. the time interval is not distinguishable. The mean value is assumed to known by adversary as he can calculate it from observed message intervals and seed is kept secret.

Algorithm 2 of Goodness of Fit Test with proper delay is introduced to confirm the random distribution is followed at the output. The input is a series of data packets and the output should be in a random distribution. The algorithm's base idea is to consider the series in order to judge the distance distribution between the data. The execution of algorithm 1 gives a random traffic followed by all signals i.e. carrying fake message also carrying real message. The technique used while transmitting the real and fake messages is- the random number selected is divided by number of nodes set and taken a mod value, if mod value is zero then transmits real message; otherwise, fake message. Thus traffic embeds both fake and real message series.

Algorithm 2: Goodness of Fit Test with proper delay
Input: a sequence of data with inter-message time intervals
Output: True, if it follows random distribution with proper delay; otherwise, false.
Procedure:
1: A random number is selected (rand / threshold)
2: if rand%20=0, send real event, otherwise, false.

When a real event occurs, its report can be embedded within the transmissions of fake messages. Transmitting real events as soon as they are detected does not provide source anonymity against statistical adversaries and to mitigate the

above statistical analysis they can be transmitted instead of the next scheduled fake one. This however, introduces additional delay before a real event is reported but when real events have time sensitive information it might be unacceptable, Transmitting highly confidential data may adopt this approach.

The challenge, however, is to develop a model that captures all possible sources of information leakage and a proper way of quantifying anonymity in different systems. As SAS model provides strong source anonymity in WSN and meets the limitation of other existing solutions this is the best method suited for achieving source anonymity.

Algorithm 4: Implementing LSB technique
Input: Least significant bit with data packet to be transmitted
Output: Data forwarded to true address or forwarded randomly
Procedure:
1: Apply LSB
2: if source port i.e. LSB bit in source data is 1 then data forwarded to the address in the packet embedded
3: if 0 then data forwarded randomly in network.

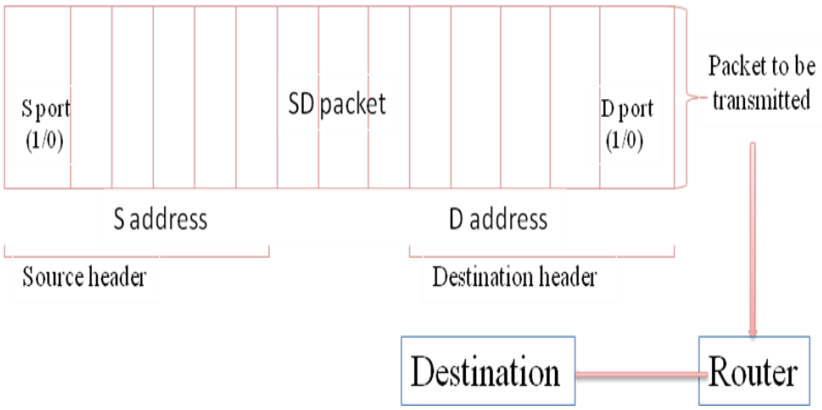

Fig.1: LSB Steganography as a source signature

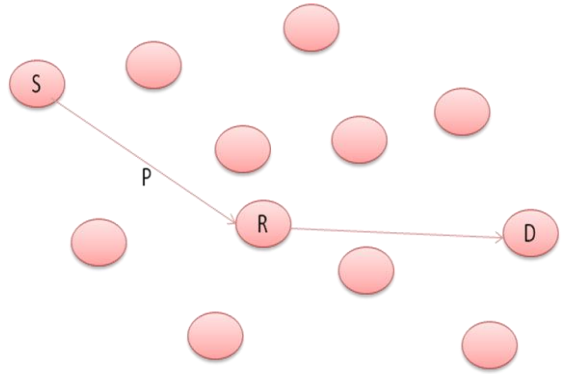

Fig.2(a)

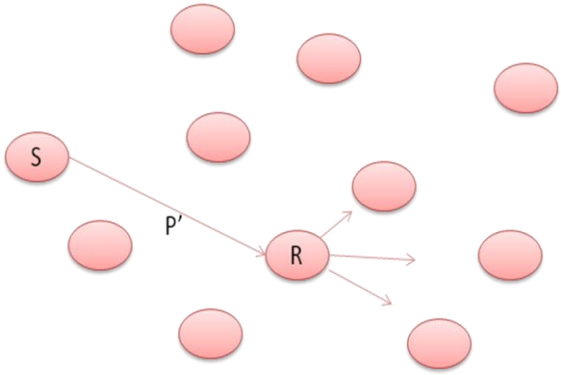

Fig.2(b)

[Figure 2 represents data transmission from source to destination, where S- source D-destination R-router P-packet with sport+dport=01 and P'-packet with sport+dport ! =01].

For acquiring better results the combination of LSB with steganography and source signature is introduced i.e. source signature is implemented using LSB steganography. The source signature is implemented by embedding the SD packet within sender signature (SS) header and sender signature tail where each packet of header and tail will be masked with 4 bits data as signature. The packet transferring from source to destination will carry SS header, source address, SD packet, destination address, SS tail. The port number of source will be embedded as head and tail working as a signature. If port number will be +1 then router routing the data packet will route it to the address in the packet and if port number will be -1then the data packet will be randomly distributed in the network. Thus the least bit works here as a signature hiding the actual transformation information.

The system flow diagram shown in figure 3 represents the working of the system in order to achieve its goal of source anonymity following EI and II with nuisance parameter. The AODV protocol used to transmit the data is a routing protocol and hence our actual code file i.e.aodv.cc file is installed at router. The router has all the node information in its network. The system first forms the network with fixed initialised number of nodes. The system requires the source and destination to be carrying communication. It randomly then generates the threshold value and counter is set. The threshold value mod with number of nodes if equal to 00 then forwards true packet otherwise the fake packet is transmitted randomly in network. If number of packets to be transmitted is complete then it again follows same procedure with set of source and destination value otherwise it continues with different random number generating to send real and fake message series in the network.

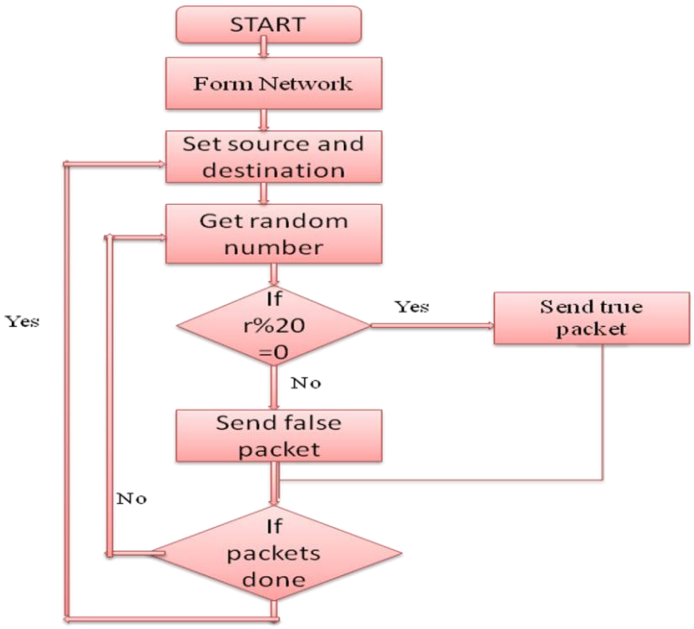

Fig.3: System Flow Diagram

III. SIMULATION RESULTS

The system code execution first enables us with the network formation which is the simulated form of wireless sensor network shown in figure 4. If algorithm is applied then the output is of real and fake messages with threshold value operated and in accordance of that threshold value the transmission of real and fake signal is done, shown in figure 5. If algorithm is not applied then the traffic contains real transmissions and in simulation's NAM file shows the real node transmitting the data to desired destination.

Figure 6 (a) and (b) shows the simulation output of energy without algorithm and with algorithm respectively. The x-axis represents simulation time in millisecond and y-axis carrying energy required in joules. The energy required to transmit the data from source to destination with algorithm implemented is not much high and nearly equal even in comparison little less energy is required.

Figure 7 shows throughput result of packet transmitted without algorithm implemented and with algorithm in (b) and (a) respectively. Throughput i.e. successful packet delivered at the destination. X-axis carrying simulation time and y-axis having packet delivered ratio. Implementing this technique resulted in constant ratio of packet delivery

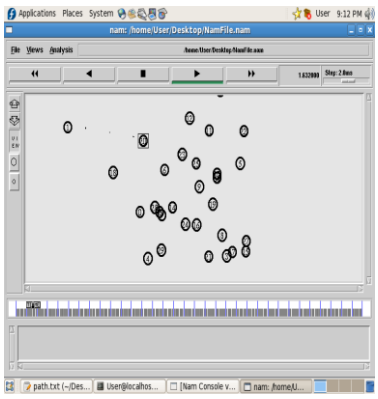

Fig.-4: network formation

```
T:Sending packet from Node 1 at port 0 to Node 5 at Port 0
Packet Threshold 20
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 13
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 10
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 14
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 4
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 24
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 4
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1


T:Sending packet from Node 1 at port 0 to Node 5 at Port 0
Packet Threshold 17
F:Sending packet from Node 0 at port 1 to Node 6 at Port 1
Packet Threshold 26
```

Fig.5: traffic output with algo.

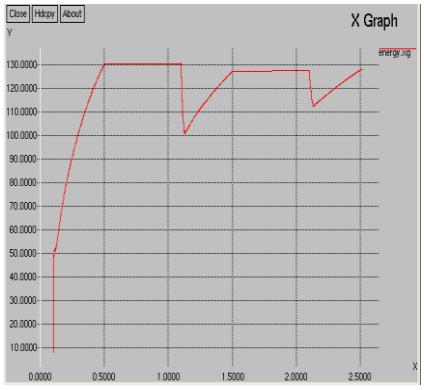

Fig.6 (a): Energy output without algorithm

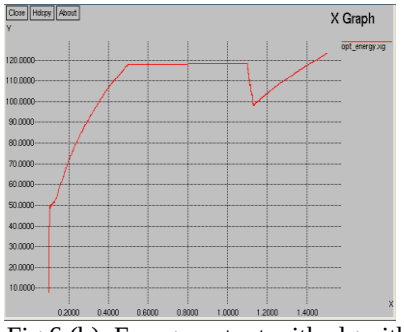

Fig.6 (b): Energy output with algorithm

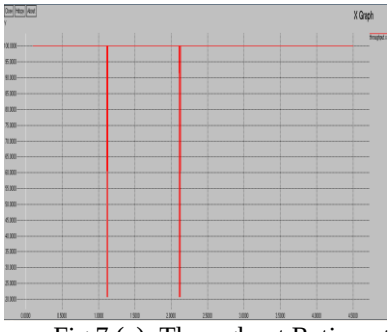

Fig.7 (a): Throughput Ratio output Without algo

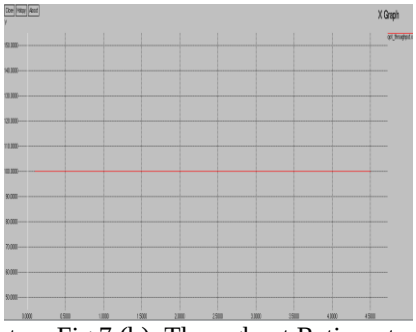

Fig.7 (b): Throughput Ratio output with algo

IV. CONCLUSION

After analyzing the source anonymity problem under the global attacker model, identification of the fundamental tradeoff between performance and privacy is done. The notion of statistically strong source anonymity for sensor networks meets the requirements strongly. Performance evaluations demonstrate that, by this scheme, the event report latency is largely reduced and source location privacy is preserved even if the attacker conducts various statistical tests.

The coding theory and mapping of statistical problem with nuisance parameter is carried. Quantification of statistical source anonymity is done by noting the number of fake signals and real, carrying out its average value.

REFERENCES

[1] Rupali D. Shinganjude, Deepti P. Theng, "Inspecting the ways of source anonymity in Wireless Sensor Network" I.C. Communication System and Network Technologies -2014.
[2] Mauro Conti, Jeroen Willemsen, and Bruno Crispo "Providing Source Location Privacy in Wireless Sensor Networks: A Survey" IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013.
[3] Jon R. Ward and Mohamed Younis "On the Use of Distributed Beam forming to Increase Base Station Anonymity in Wireless Sensor Networks," 2013 IEEE.
[4] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a Statistical Framework for Source Anonymity in Sensor Network", IEEE Transactions on Mobile Computing, February-2013.
[5] Bidi Ying, Jose R. Gallardo, Dimitrios Makrakis, Hussein T. Mouftah "Concealing of the Sink Location in WSNs by Artificially Homogenizing Traffic Intensity", 2011 IEEE.
[6] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "On Source Anonymity in Wireless Sensor Networks," IEEE Computer Society, 2010.
[7] "Statistical Framework for Source Anonymity in Sensor Networks," IEEE Communications Society, 2010.
[8] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-layer Enhanced Source Location Privacy in Sensor Networks," IEEE SECON, 2009
[9] Q.Gu, X. Chen, Z. Jiang, and J. Wu, "Sink-Anonymity Mobility Control in Wireless Sensor Networks," Wireless and Mobile Computing, Networking and Comm., 2009.
[10] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," IEEE Communications Society, 2008
[11] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, 2008.
[12] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," IEEE Computer Society, 2007.
[13] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source Location Privacy in Sensor Network Routing," IEEE Computer Society, 2005.
[14] C. Ozturk, Y. Zhang and W. Trappe, "Source-location privacy in energy constrained sensor network routing," in SASN, 2004.
[15] D.Niculescu and B.Nath "Trajectory Based Forwarding and its Applications", MobiCom-2003. Wang; Chow, S.S.M.; Qian Wang; KuiRen; Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Computers, IEEE Transactions Feb. 2013.Wang; Chow, S.S.M.; Qian Wang; KuiRen; Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Computers, IEEE Transactions Feb. 2013.
[16] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P. Reddy,"Implementation of LSB Steganography and its Evaluation for Various File Formats", I.J Advanced Networking and Applications,(2011).

