ROBUST ENCRYPTION ALGORITHM BASED SHT IN WIRELESS SENSOR NETWORKS

Uma.G and Sriram.G

Department of Electronics & Communication Engineering, Parisutham Institute of Technology, Thanjavur, Tamilnadu, India

ABSTRACT

In bound applications, the locations of events reportable by a device network have to be compelled to stay anonymous. That is, unauthorized observers should be unable to notice the origin of such events by analyzing the network traffic. I analyze 2 forms of downsides: Communication overhead and machine load problem. During this paper, I gift a brand new framework for modeling, analyzing, and evaluating obscurity in device networks. The novelty of the proposed framework is twofold: initial, it introduces the notion of "interval indistinguishability" and provides a quantitative live to model obscurity in wireless device networks; second, it maps supply obscurity to the applied mathematics downside I showed that the present approaches for coming up with statistically anonymous systems introduce correlation in real intervals whereas faux area unit unrelated. I show however mapping supply obscurity to consecutive hypothesis testing with nuisance Parameters ends up in changing the matter of exposing non-public supply data into checking out associate degree applicable knowledge transformation that removes or minimize the impact of the nuisance data victimization sturdy cryptography algorithmic rule. By doing therefore, I remodel the matter of analyzing real valued sample points to binary codes, that opens the door for committal to writing theory to be incorporated into the study of anonymous networks. In existing work, unable to notice unauthorized observer in network traffic. However our work in the main supported enhances their supply obscurity against correlation check. the most goal of supply location privacy is to cover the existence of real events.

KEYWORDS

source location, privacy, anonymity, consecutive hypothesis testing, sturdy cryptography algorithmic rule, nuisance parameters.

1. INTRODUCTION

A Wireless Sensor networks is a network comprising of nodes that are connected wirelessly and communicate with each other. Wireless sensor network remains one of the challenging research domains. Sensor networks are used in several applications such as military, healthcare, monitoring purposes and surveillance. Sensor networks provide time and location privacy and it is better suited to physical environment. Nodes are used to transmit information when an event is detected. SENSOR networks are deployed to sense, monitor, and report events of interest in a very wide selection of applications as well as, however don't seem to be restricted to military, health care, and animal chase. There are measure 3 parameters that may be related to an occurrence detected and according by a device node: the description of the event, the time of the event, and the location of the event.

Once device networks are deployed in untrusty environments, protective the privacy of the 3 parameters that may be attributed to an occurrence triggered transmission becomes a vital security feature within the style of wireless device networks. The source anonymity downside in wireless device networks is that the downside of learning techniques that offer time and placement privacy for events according by device nodes. Time and placement privacy are used interchangeably with supply anonymity throughout the paper.

Within the existing literature, the source namelessness problem has been self-addressed beneath 2 differing types of adversaries, namely, local and international adversaries. an area opponent is outlined to be associate opponent having restricted quality and partial read of the network traffic. Routing primarily based techniques are shown to be effective out of sight the locations of according events against native adversaries. A global soul has the ability to monitor the traffic of the complete network (e.g., coordinative adversaries spatially distributed over the network).

Against international adversaries, routing primarily based techniques are to be ineffective in concealing location data in event-triggered transmission. this is often as a result of the actual fact that, since a worldwide soul has full abstraction read of the network, it will straight off sight the origin and time of the event triggered transmission. We have a tendency to introduce the notion of "interval identicalness" and illustrate how the matter of applied math supply namelessness will be mapped to the matter of interval indistinguishability. Nodes are deployed to sense events of interest and report them with minimum delay. Consequently, given the placement of a definite node, of the placement, the node of the rumored event of interest will be approximated. Within the node‟s communication vary at the time of transmission. When a node senses an occasion, it places data regarding the event in a very message and broadcast encrypted version of the message. To obscure the report of an occasion of interest, nodes square measure assumed to broadcast faux messages, even though no event of interest has been detected.

2. LITERATURE SURVEY

In this paper [2], Preserving source location privacy is becoming one of the most interesting problems in wireless sensor networks. In a variety of real life applications, such as the deployment of sensor nodes in battle fields, the locations of events monitored by the network are required to remain anonymous. Given the knowledge of the network topology, however, an adversary can expose the locations of such events by determining the individual nodes reporting them. Here real events must be delayed until the next scheduled Fake transmission. When real events have time-sensitive information, such latency might be unacceptable.

In paper [3], SPINS has two secure building blocks: SNEP and TESLA. SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication, and data freshness. Particularly hard problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. TESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. SPINS does not place any trust assumptions on the communication infrastructure, except that messages are delivered to the destination with nonzero probability.

In paper [4], a routing technique is used to provide adequate source-location privacy with low energy consumption. We introduce this technique as the Sink Toroidal Region (Star) routing. With this technique, the source node randomly selects an intermediate node within a designed

Star area located around the SINK node. The Star area is large enough to make it unpractical for an adversary to monitor the entire region. Furthermore, this routing protocol ensures that the intermediate node is neither too closes, nor too far from the SINK node in relations to the entire network. Here Network traffic and passive attack is possible.

In paper [5], they propose two techniques that prevent the leakage of location information: periodic collection and source Simulation. Periodic collection provides a high level of location privacy, while source simulation provides trade-offs between privacy, communication cost, and latency. Through analysis and simulation, we demonstrate that the proposed techniques are efficient and effective in protecting location information from the attacker. Communication problem and network traffic is the major drawback here.

In paper [6],they first formulate this privacy problem as a constrained optimization problem and then develop heuristics for an efficient privacy algorithm. Using simulations with randomized movement models we verify that the algorithm improves privacy while minimizing the perturbation of location samples.

3. EXISTING APPROACHES FOR SSA

In Existing work [1], Network coding-based approaches that protect against traffic analysis have appeared. The privacy problem most relevant to this work is the source location privacy in wireless sensor networks. The local eavesdropper model was introduced and the authors demonstrated that existing routing methods were insufficient to provide location privacy in this environment.

They also proposed a phantom flooding scheme to solve the problem. It causes source anonymity problem and does not provide source location privacy and here attack is possible. With the help of statistical hypothesis testing, they are unable detect the hacker and it results in source anonymity problem. In this system, faux and real transmission is possible. Here the inputs are taken in a random manner. So that there may be a possibility of false information.

4. PROPOSED APPROACH FOR SSA

In this paper, I propose a modification to existing solutions to improve their anonymity against correlation tests. Our work include mapping the problem of statistical source anonymity to coding theory in order to design an efficient system that satisfies the notion of interval indistinguishability.

The main goal of source location privacy is to hide the existence of real events. I am going to protect our information from attackers using sequential hypothesis testing and robust encryption algorithm. Here the information is sent from source to destination. While sending the message, the attacker may able to modify the message and send it to destination. While reaching the message to the destination, the destination may confuse about the sender who sends the message. Source anonymity problem arises. In order to overcome the drawbacks of existing approach, sequential hypothesis testing is used.

Here the inputs are taken in a sequential manner to improve the security. Then determine the correlation value and map the value to sequential hypothesis testing to remove the redundant information. For providing source location privacy, I use robust encryption algorithm to send the message to the target recipient without any interruption. In this approach, I am going to improve security and perform network security analysis in an efficient manner to reduce latency time. Here fake transmission is impossible.

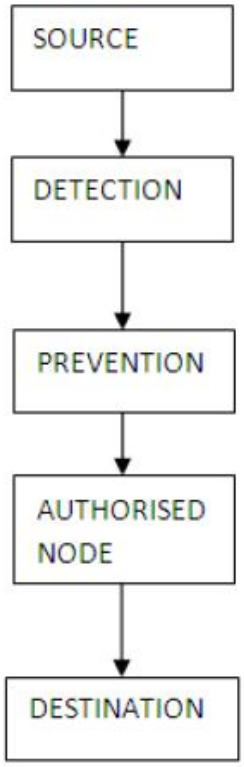

Fig 4(a): System Architecture

In figure 4(a),it consists of single input and single output. Here the information is transferred from transmitter to receiver. Each base station receives the signal from transmitter and sent to the destination. Here we consider existing system as well as proposed system. In existing system, Anderson test and binary hypothesis testing is used. But in our approach, we detect the source anonymity problem with the help of sequential hypothesis testing as well as protect our system from hackers using robust encryption algorithm.

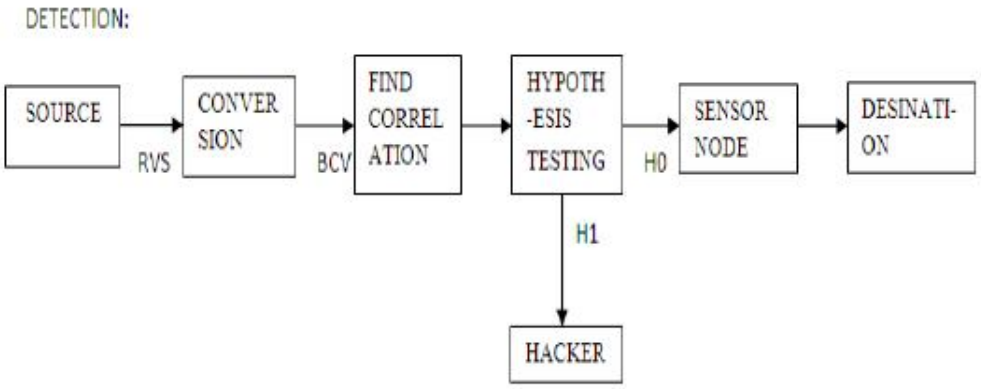

Figure shows the block diagram for detection. Here the information is continuous that the real values are converted into the binary values for identifying the noise parameters. Next we have to find the correlation value for the input data. With the help of the correlation value, it undergoes hypothesis testing to determine which the data sample belongs to. With the help of testing hypothesis, we have to determine the transmission is real or fake. If it is a fake node, attacker will be there. Here we are using sequential hypothesis testing. With the help of the above diagram, we are going to detect the hacker transmission. After detection, we have to protect our encrypted message from hackers.

5. EXPERIMENTAL ANALYSIS OF SSA BASED ON SEQUENTIAL BASED HYPOTHESIS TESTING:

The use of sequential hypothesis testing is to provide secure system against anonymous source in wireless sensor networks. Now we have to analyze the effectiveness based on experimental analysis.

Convert real valued samples into binary codes:

Let every inter transmission time is shorter than mean μ be represented as a „0" and inter transmission time is longer than mean μ be represented as „1". We have to convert the real valued samples into binary codes to remove the nuisance parameters in the information. for a given sequence X={x1,x2,…..xn},then

$$g(xi) = \begin{cases} 1, if\ x_i > \mu \\ 0, if\ x_i < \mu \end{cases} \quad \text{for each i=1,2,….n.}$$

next we describe the correlation value to set the threshold value that will be used for experimental analysis of source anonymity based on sequential hypothesis testing.

CORRELATION MEASURE FOR SOURCE ANONYMITY:

For finding correlation value, we use the sequential probability ratio test because here we consider the input sample values are taken in a sequential manner.

$$\Lambda_k = \prod_{i=1}^{k} p_1(x_i)/p_0(x_i) \quad \text{For k=1,2,....n}$$

It can be verified that the value of correlation should be in the range 0 to 1. The goal of the SPRT is to decide which hypothesis is correct as soon as possible (i.e., for the smallest value of k). To do this the SPRT requires two thresholds, $\gamma 1 > \gamma 0$. The SPRT stops as soon as $k > \gamma 1$, and we then decide H1 is correct, or when $k <= \gamma 0$, and we then decide H0 is correct. The key is to set the thresholds so that we are guaranteed a certain levels of error. Making 1 larger and 0 smaller yields a test that will tend to stop later and produce more accurate decisions. We will try to set the thresholds to provide desired probabilities of detection PD and false-alarm P_{FA}.

With the help of SPRT, we are going to detect attacker in the system. If we perform hypothesis testing, we need test statistic value,. If the test statistic value is greater than 0.01, then the network will be more secure otherwise there may be a possibility of attacker. Using hypothesis testing, we are going to detect the hacker in our wireless sensor network. Here we can overcome the problem of computational overhead and communication overhead. By using sequential hypothesis testing, we have to reduce source anonymity problem.

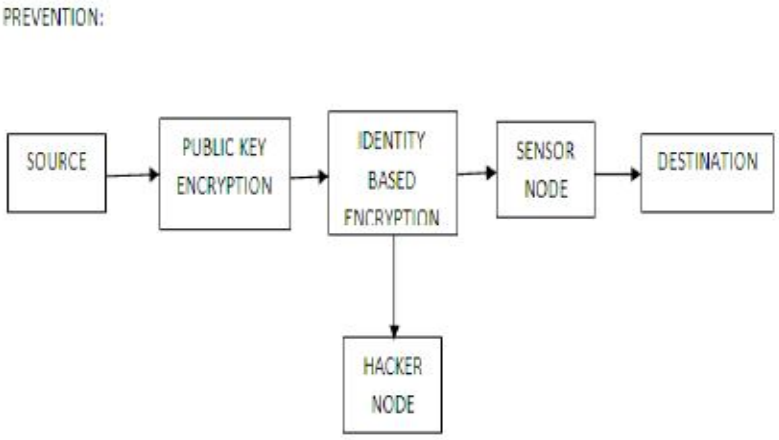

Figure 5(a) shows the mechanism of protecting our information from hackers. For that we require public key encryption and identity based encryption. Here the message is encrypted and identity based encryption is used to identify the target recipient. Here we consider the target recipient as sensor node. Then the message will reach to destination. Here in prevention, packet broadcasting is most important factor in wireless sensor networks. Here messages are divided into packet and packets are encrypted and send in a sequential manner. The information will send to the particular target recipient using identity based encryption.

6. RESULT ANALYSIS

In wireless sensor networks, first we create a node between source and destination. Nodes are to be active when the information is transmitted from source to destination. Nodes are communicated in a wireless medium. We have to create any number of nodes.

Mesh topology is used for secure communication compare to all other network topology. Here we are having detection and protection techniques. The experimental results showed that how to create nodes and how the message is transferred from source to destination and the methodology used for detection.

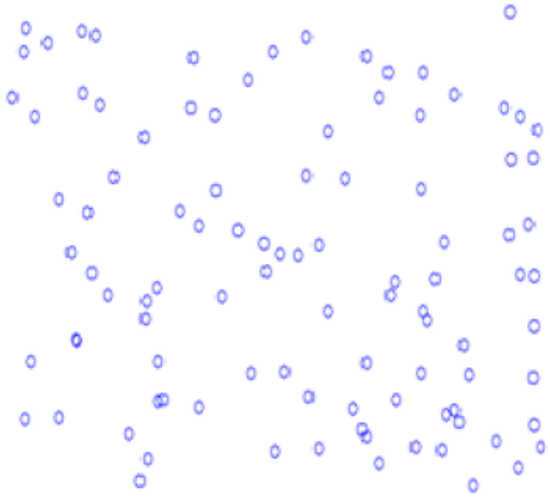

Fig 6(a): node creation

In fig 6(a), the nodes are created and the information can sent through the node. Nodes are used for monitoring purposes. In our next step, the message can be passed through the sensor nodes present in the network. Here we are using mesh topology for secured communication.

Mesh topology is used to connect networks in a wireless medium. Nodes are used to sense the events takes place in the sensor networks and it will describe the event and time of the event. Next step in source anonymity is the message passing from source to destination .then message can be passed through the sensor node that can easily communicate through radiowaves.it can easily observe the encrypted message and check the target recipient and the message is sent to the receiver. It is an efficient system and it detects the unauthorized observer present in wireless sensor networks.

In previous case, they are unable to detect the hacker. They can take the input in a random manner. So noise will be more and there will be a computational overhead and communication overhead. In order to reduce the above problem, we are going for message passing and detection.

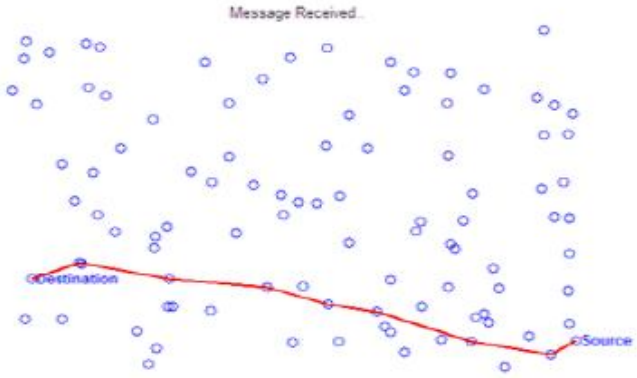

Fig 6(b): message passing

In fig 6(b), the message is encrypted and the message is divided into packets and the packets are sent in a sequential manner in order to reduce the communication overhead and computational load problem. The message can reach the destination in secure manner.

In the above graph, message can sent from source to destination. In between them, sensor nodes between them. Message can be transmitted in a wireless medium. In sensor networks, there may be a possibility of attack. This attack can results in modification of message, masquerade and disclosure. In order to detect hacker in this system, we go for sequential hypothesis testing in order to design an efficient system. in our next step, we have to provide source location privacy and to reduce the network traffic. Secure communication is possible.

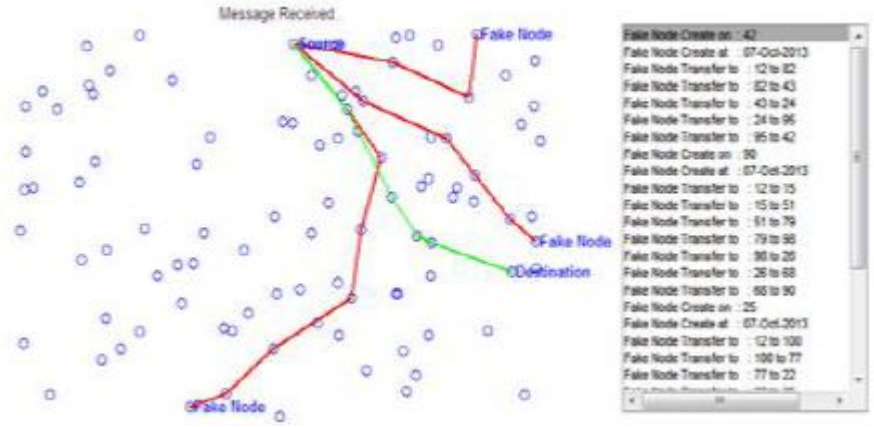

Fig 6(c): detection of hacker node when information is transmitting from source to destination.

For finding the shortest path we use djikistra algorithm and detect there may be any hacker node using sequential hypothesis testing. In the above graph, we have to identify the number of fake nodes during transmission. This solution is merely presented how to reduce source anonymity problem based on sequential hypothesis testing. Using the proposed framework, including the mapping of source anonymity to sequential hypothesis testing in order to design the notion of interval indistinguishability. Fake events are identified. The main goal is to reduce latency and to

reduce network traffic. SPRT is the only choice to detect fake event. Hence the attacker is unable to hack the original information .our system must be more secure by considering correlation tests.

7. CONCLUSIONS

In this paper, we provided a framework for source anonymity based on sequential based hypothesis testing. We introduce the notion of interval indistinguishability to provide source location privacy. By mapping the problem of source anonymity to sequential hypothesis testing in order to design an efficient system. We showed why previous studies are unable to detect attacker. Finally we propose a modification in the existing system to reduce network traffic.

REFERENCES

[1] Basel Alomair, Member, Andrew Clark, Jorge Cuellar, and Radha Poovendran, "Towards Statistical framework for source anonymity in wireless sensor networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013

[2] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "On Source Anonymity in Wireless Sensor Networks," Proc. IEEE/IFIP 40th Int"l Conf. Dependable Systems and Networks (DSN "10), 2010.

[3] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8,no. 5, pp. 521-534, 2002.

[4] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE 15th Int"l Conf. Network Protocols (ICNP "07), pp. 314-323, 2007.

[5] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," Proc. IEEE/CreatNet First Int"l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm "05), pp. 194-205, 2005.

[6] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey," Elsevier J. Ad Hoc Networks, vol. 7, no. 8, pp. 1501-1514,2009

[7] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, pp. 466-474, 2008.

Author

Uma.G was studying M.E-Communication Systems in Parisutham Institute Of Technology and Science,Thanjavur,Tamilnadu, India. (Affliated to Anna University).