Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security for Source Node Privacy in Wireless Sensor Network

Devdatt Nadre, Balaso N. Jagdale
Department of Information Technology
MIT College of Engineering
Pune, Maharashtra, India

Abstract—Source location privacy is one of the most challenging topics in security WSN. Wireless Sensor Networks have been widely used in many areas for various infrastructure monitoring, tracking and information collection. We are generated more fake node, fake packet and to create anonymity node for source location privacy. They are providing privacy to the event detecting, tracking sensor node and integrity to the data gathered by the sensor node. Sensor Network uses random walk path or generates more fake event packets for adversary. We may difficult to trace packet and location for an adversary to detect real identity in environment. We are providing security from Eavesdropping attack, black-hole node, misbehaving, Denial of service, compromise attack and packet spoofing. We are used SPENA model for identify various attacks on sensor network and evaluate impact of attack. It is provided source node privacy under attacks using SPENA approach. We are finding impact of attack on network using attacks concept and improve security using security techniques. We optimizes packet delivery ratio, energy consumption, packet drop rate, packet delay, message collisions, achieved privacy functionality and calculate performance metrics.

Keyword—Wireless sensor network privacy, Source location privacy preserving scheme, attacks, context privacy, performance optimization.

I. INTRODUCTION

Wireless sensor network have significant to different field military surveillance application, personal health monitoring, tracking endangered species and civilian application. It has limited storage, computing power, and battery life.WSN nodes can be categorized as source node, sink node and intermediate nodes depending upon functionality in environment. Context source node is that node to transmission of some kind of information as reaction to some event occurring in its sensing range. Intermediate node is used as data forwarders in multi hop communication [1]. Sink node is control all over node that node present in sensing range and Sink gathers the sensed data from the entire nearby node for final processing. Sensor network may be categorized broadly into Content privacy and context privacy threats. Content privacy threats generate due to the ability of the adversary to track, observe and manipulate the exact content of packet being sent over on sensor network. Context privacy is concerned with protecting the context associated with the sampling and transmission of sensed data. Context privacy can be used for location of the source node. SPENA model is protected source location privacy under eavesdropping and node compromises attacks. The selective forwarding attack is difficult to detect, since communication networks are unreliable, where is a loss of number of packet in transmission period. It can create secure environment in sensor area from various attacks and adversary [2].

We are interested in tracking and monitoring application, such as tracking animal activity and monitoring the movement of doctor and patient. Source privacy is generally compromised by Meta and contextual information on source node through packet. Adversary node can be send packet at real node and try to find credential information for misuse purpose. Let us take about the well known panda hunter game as an example source node is sending packet any direction in environment to find object. It is find location, time of panda to detect in a sensed area. Node sense panda informs the sink by sending massage travels through intermediate node to the sink node. It also find hunter position in environment for protect the panda from the hunter. A similar problem happen in other application such as monitoring the patient and doctor in a hospital and tracking friendly soldier on the battlefield .they protect subject from the adversary. It must hide the location of the source that senses the subject. Source location privacy requires more than confidentiality of the message exchanged between nodes. The confidentiality of message is part of another privacy category, called content privacy. Content privacy gives important on providing integrity, non repudiation and confidentiality of the message exchange in sensor network. Context privacy comprises, for instance, hiding the identity and the location of each node and hiding the traffic flow in between different node. [3]

II. SOLUTION AND IMPACT OF ATTACKS SOURCE LOCATION PRIVACY

1. Solution for Source location privacy:

We define set of categories based on the solution for providing source location privacy. They first discuss following different categories namely: fake node and Dummy packet, cluster Anonymization, routing based source location privacy, flooding based approach etc. And second scenario, we discuss about impact of various threats dividing different categories namely: adversary, eavesdropping, node compromise, black hole attacks etc. We are analyzed security in attack affected network area.

A. Fake Node and Dummy packets

Their first technique uses fake source with that node sending fake event packets to confuse the adversary. Fake event is basically a dummy message that message is created by another node than a source location. Fake node is sent message request at real node to capture credential information. Sometime adversary does not know which real packet to follow. Fake source node is injecting fake message into network and thus diffuse the source of message. It is using flooding protocol to generate more fake packet in network. Fake node has been created fake node identity and packet does not mention any source and destination identity. It is randomly transmitted any direction in sensor area. content privacy threats generate due to the ability of the adversary to observe and manipulate the content of packet being sent over the wireless sensor network .It is efficiently create fake source and define the optimal message generation rate. Flooding technique is energy consuming and there is the possibility of adversary backtracking to the source node. Real node can use cryptography technique for source location privacy [2, 14].

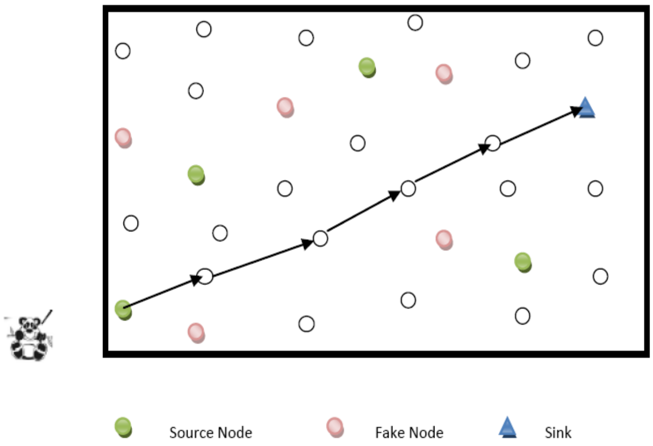

Figure 1: Fake node and packet

B. Cluster Based Anonymization

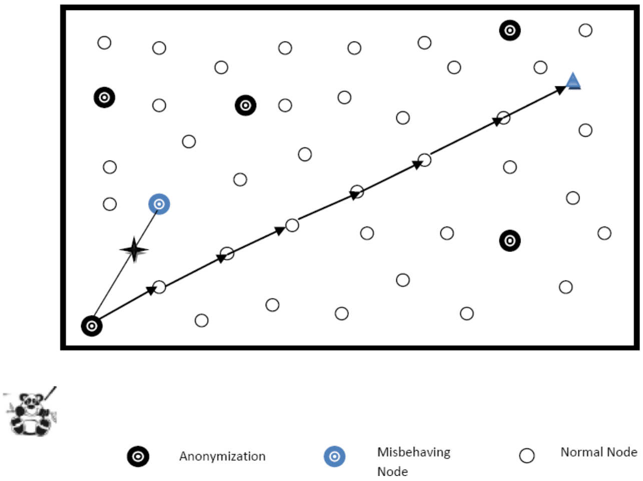

Figure 2: Cluster based anonymization

It is used for to hide real identity for source node and packet over network. It gives random identity for each and every source node in sensor area. Adversary finds out the source ID by reading the header information, but adversary cannot find real identity .It gets to know only the pseudo identity number which is not linked with source location. Adversary cannot distinguish a source in the observed area. There are divided in different category namely packet anonymization, cluster based anonymity, hash based randomization, cryptographic technique anonymity. Source location anonymity have own identity to represent divert for adversary [4, 14].

C. Routing based source location privacy

It develops a model to quantitatively measure source location credential information leakage for routing based source location privacy schema. The main idea is to protect the adversaries from tracing back to the source location through traffic monitoring and analysis. Routing based protocol is the phantom routing protocol. It is used two phase routing schema to protect routing based source location information. Message is selected random path forward to actual destination node. Direction information must be stored in the messages header. Intermediate node is selected random path to transfer next forward node on the routing path along the same direction. Adversary can trace message on network mixing ring using fake packet. It possible for adversary to monitor and link all message from the same source node which may help the adversary to identify the source location, ID is corresponding to the grid location [5].

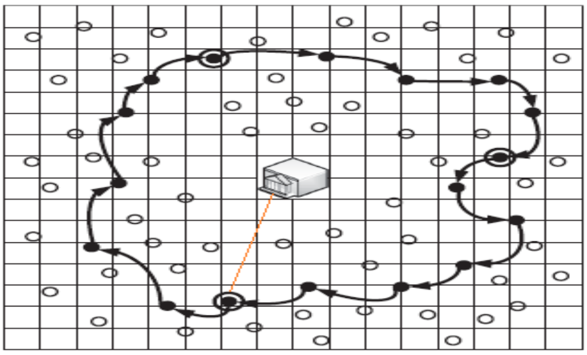

Figure .3: grid information

D. Flooding based techniques

Flooding based routing is handled various packet flow in Sensor environment. It posed various security problems in sensor network for example link failure, collision, network jamming and packet loss ratio increases. Techniques are usually easy to implement since simplifies the routing protocol. The communication cost of message flooding might be prohibitively expensive in WSNs. for flooding based approach it should be generate fake packet traffic to confuse for local and global adversary. [6]

E. Single path routing

It mentions criteria to quantitatively measure source location message leakage in single routing based source location privacy schemes for WSN's. It is energy efficient routing techniques allow a node to forward packets only to one of its neighbors. Single-path routing techniques usually require either extra hardware support or a pre-configuration phase. It's nearest neighbors and the destination to calculate a greedy single routing path. There are number following technique to maintain flow and source privacy: trajectory based routing, directed diffusion [7].

2. Impact of attack in source location privacy:

We are categories different attack happen on wireless sensor network to provide source location privacy. In Some condition various attacks reduce network performance but fake nodes are protected real data from those attacks. There are following attack show various impact on network namely: adversary, eavesdropper, compromise nodes, packet spoofing, and Black hole attack.

A. Adversary attack

Adversary can drop number of packets in simulation time. It can insert its own packets into the network. Internal adversary can compromise a node within the sensor area. Whereas an external adversary cannot do that .internal adversary has access to components and an external adversary does not have permission to access. The active attacks of the adversary comprise injecting false packet into the dropping actual packet network traffic. Passive attack is eavesdropping in which adversary listens to the traffic and tries to capture the content that is exchange between at node. A semi honest adversary follows the protocol within the WSN to ensure that it remain unidentified as an adversary while a dishonest adversary does not comply with the protocol within the sensor network. Semi honest is compliant with the protocol and dishonest is not compliant. [2, 4]

B. Eavesdropping

The Eavesdropping attack is a serious security threat to a sensor network. Conventional sensor area consist of wireless nodes equipped with Omni-directional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. For Passive Eavesdropping in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium. For Active eavesdropping where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. For eavesdropping attacks they are using cluster based anonymization techniques to protect from those attacks [2, 11].

C. Compromise node

Adversary uses a compromised node to influence the protocol or to detect other node .adversary can also destroy a node in this case. Adversary uses a compromised node to get information such as the identity of a node, the information received and sent by node and encrypt keys of a node. Compromise node can send packet to real node to access data unauthorized way. On that node they can access data from different node. Fake node used for to confuse compromise node packet attack in sensor area [1, 2].

D. Black hole attack

A packet drop attack or black hole attack is a type of denial of service attack accomplished by dropping packets. A black hole attack is an attack that is mounted by an external adversary on a subset of the sensor nodes in the network.

When the source select the path including the attacker node, the traffic starts passing through the adversary node and this nodes starts continuous dropping the packets selectively or in whole. Reprogrammed nodes are termed as black hole nodes and the region containing the black-hole nodes are black hole region. Black hole region is the entry point to a large number of harmful attacks [15]

III. LITERATURE SERVEY

Earlier papers are describing to provide source location privacy using various approaches is discussed below.

In next techniques [1, 13], anonymous concept is used to hide real identity from adversary node attacks. To preserve source location privacy becomes important in wireless sensor network .the privacy threat occur for sensor networks may be divide in different category into content privacy and context privacy. Those techniques are used to hide sensitive information in source location privacy. They are proposed a source location privacy scheme for WSN through cluster based anonymization. It must be hide real identity during communication. Entropy based method is used to find degree of privacy.

Kantha Kumar Pongaliur et al [2] also introduced a sensor networks use either select random path or generate number of fake event packet to make it hard for an adversary to track real identity. They mention that hiding source information using cryptographic techniques incurring lower overhead. The adversary model considers a super local eavesdropper having the ability to compromise sensor node. They are provided source privacy under eavesdropping and node compromise attacks using SPENA model. They use a one way hash chain based keying mechanism to hide the source information.

Mauro conti et al [3], they provide a survey of state in source location privacy. It mentions key concepts in source location privacy, such as anonymity, unobservability, and safety period and capture likelihood.

In this paper [4], they proposed a solution for the source location privacy from information leakage problem. They propose to quantitatively measure source location information leakage in routing based source location privacy. They identify vulnerabilities of some well known source location privacy protected schemes. They are mention to provide source location privacy through routing to a randomly selected intermediate node and network mixing ring. That aim to provide excellent SLP under adversary attacks.

In next techniques [5, 2], they proposed a new framework for modeling, analyzing, and evaluating anonymity in sensor networks. We introduce the notion of interval indistinguishability and provide a quantitative measure to model anonymity in sensor networks; we maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. They analyze existing solutions for designing anonymous sensor networks using the proposed model. To solve how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information.

Mohamed M.E.A. Mahmoud and Xuemin Shen ,[6] they first proposed a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to the large volume of packets originating from a small area. Second, they develop a realistic adversary model, assuming that the adversary can monitor the network traffic in multiple sensor areas. They introduce a novel attack called Hotspot Locating where the adversary uses traffic analysis techniques to locate hotspots. a cloud based scheme for efficiently protecting source nodes location privacy against Hotspot Locating attack by creating a cloud with an flexible shape of fake traffic generate, counteract the inconsistency in the Traffic pattern and camouflage the source node in the nodes forming the cloud.

Jian Li, Yun Li, Jian Ren, [7] proposed schema based on either symmetric key cryptosystems or public key cryptosystems. They propose a scalable authentication scheme based on elliptic curve cryptography. They allow any node to transmit an unlimited number of messages without suffering the threshold problem. They can also provide message source privacy. That scheme is more efficient than the polynomial based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy

They investigated approach for they define a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to in a small range area a large number of data is initializing. [8], they develop a realistic adversary model, considering that the adversary can monitor the network traffic in multiple area or entire network.

IV. PROPOSED SCHEME

For source location privacy, we are using fake node, fake packet to provide confusion for adversary. It can provide interlink in between different source node. All nodes are gather information for sink node. Sink node is controlled all over source node. Sink can send message to source node for sending dummy packet at adversary side .We can deploy various attacks in environment and to check impact of attack. We can build performance metric table to show all affected parameter in sensor area. We are mention important scenario in given below:

A. Confuse adversary using fake node and fake packet

We are using SPENA model to provide security from adversary and attack. It is used source node, intermediate node and sink node for initial stage to deploy in environment. We are also deployed various malicious node, faulty node to create attack affected environment for drop packet in transmission time. They are created fake node, fake packet for security point of view. Adversaries are confused to detect real node and trace real packet in environment. In this scheme they show passive adversary attack happen in environment. First technique uses fake sources, with nodes sending fake event packets to confuse the adversary. It should be analysis impact of those attacks and using adversary concept. It is detected attacker in environment to send packet at fake source node to confuse for adversary. It can find attacker position and identity in sensor area. Fake node gives wrong information to adversary for privacy. Adversary is difficult to trace real information in environment. Sink node can store information related to all node in sensor area. Fake node and fake packet present in environment to calculate performance matrices and impact of attacks. It is calculate and analysis packet delivery ratio and energy consumption. They are monitoring impact of energy consumption using fake node and packet. [1, 2, 5]

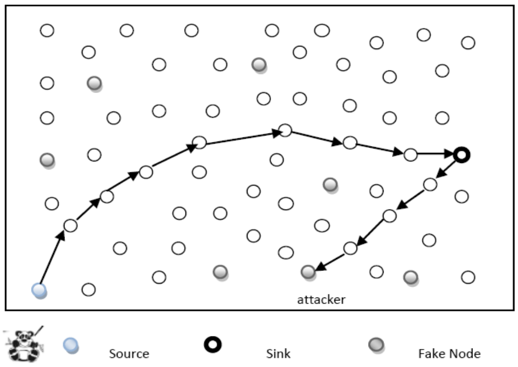

Figure 4: Privacy design Architecture

B. Source privacy Under attacks

Our aim is to maintain source privacy under compromise node, eavesdropping, misbehaving node and black hole node. We are using quadrant techniques for avoid packet collision overhead. Simulation is divided into equal partition and each quadrant has its own head node to control all quadrant nodes. We check impact of attacks in network using source location privacy concept. Misbehaving node is tried to send packet at real node and capture information from that node .fake node hasn’t trace any real identity of neighbouring real node. Fake nodes don’t give any identity and not interlink in between to each other. It is presented as part of the SPENA protocol for working in a single routing as well as a flooding based approach. We can analysis various outcome using SPENA concept.

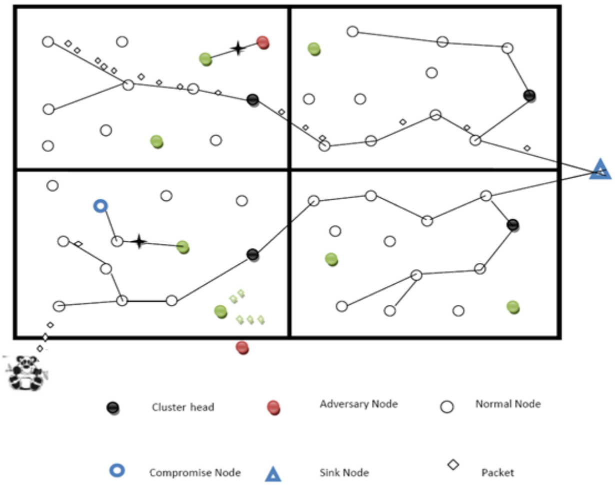

Figure 5: Privacy under attacks design Architecture

Main objective of source location privacy using SPENA model is:

- To measure energy consumption.
- To improve accuracy, data confidentiality in secure WSN.
- To impact network density using fake node and fake packet.
- To check the performances under attacks and evaluate performance metrics.
- To achieve high message delivery ratio, packet drop ratio.
-

IV. CONCLUSION

Source location of the sensor node generating the event is important in network. We can give away the event occurrence location and time. We will be made more efficient SPENA model using fake node and fake packet concept. It takes advantage of the algorithm to make the behavior of the fake sources more similar to the real ones. It is a challenge of the fake source to simulate the behavior of the real one. It can protect source privacy under eavesdropping attacks while also avoided node compromise attacks are presented. Node compromise area identification method is presented in the form of the SPENA protocol. They analyze our protocol under different attack scenarios and evaluate. Simulation results demonstrate that proposed schema can achieve very good performance in energy consumption, memory consumption and message delivery latency, while assuring a high message delivery ratio.

REFERANCES

[1] Aparna Gurjar,A R Bhagat Patil,"Cluster based Anonymization for Source location privacy in wireless sensor Network" International Conference-2013

[2] Kantha Kumar Pongaliur and Li Xiao,"Sensor Node Source Privacy and Packet Recovery under Eavesdropping and Node Compromise Attacks ", ACM Trans-July 2013.

[3] Mauro Conti, Jeroen Willemsen, and Bruno Crispo,"Providing Source Location Privacy in Wireless Sensor Networks: A Survey" IEEE Communications Survey & Tutorials, 2013

[4] Basel Alomair, Member, Andrew Clark, Student Member, Jorge Cuellar and Radha Poovendran"Toward a Statistical Framework for Source Anonymity in Sensor Networks", , IEEE, Transactions ,FEBRUARY 2013.

[5] Yun Li, Jian Ren,"Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks" IEEE, 2012

[6] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Cloud Based Scheme for Protecting Source Location Privacy against Hotspot- Locating Attack in Wireless Sensor Networks" Fellow, IEEE Transactions, October 2012.

[7] Shehla S Rana, Nitin H. Vaidya "A new 'Direction' for Source Location Privacy in Wireless Sensor Networks".

[8] Wei Tan, Ke Xu, Senior Member, IEEE, and Dan Wang,"An anti-tracking source-location privacy protection protocol in WSNs based on path extension" IEEE,2012

[9] Rongxing Lu, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE, Transactions, MARCH 2013.

[10] Jian Li, Yun Li, Jian Ren," Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" Senior Member, IEEE, Transactions ,MAY 2014.

[11] Wuchen XIAO, Hua ZHANG, Qiaoyan WEN, Wenmin LI, "Passive RFID-Supported Source Location Privacy Preservation against Global Eavesdroppers in WSN", IEEE IC-BNMT2013.

[12] Long1, Mianxiong Dong2, Kaortu Ota3, And Anfeng Liu1, "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks" ,2014.

[13] Yun Li and Jian Ren "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks" IEEE INFOCOM 2010.

[14] Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk "Enhancing Source-Location Privacy in Sensor Network Routing"

[15] Nitesh Gondwal, Chander Diwaker "Detecting Blackhole Attack in WSN by check Agent using Multiple Base Stations"international journal 2013