RESEARCH ARTICLE OPEN ACCESS

"SOURCE PRIVACY" THROUGH SELECTION OF SET AND LIVELY ROUTING PATH

G.B.Karthik Ragu[1], K.Supriya(Assistant professor- CSE)[2]

M.E Computer Science and Engineering, Apollo Engineering College

Poonamalle, Chennai

------------------*****************-------------

ABSTRACT

Wireless sensor networks (WSNs) is a large collection of sensor nodes with sensing, computational and wireless capabilities that have limited power supply and constrained computational capability. Due to dispensed nature of these networks they are easily vulnerable to numerous security threats that can adversely affect the proper functioning.The location of the source can be revealed by analysis of the direction traffic flow in the network, so the Traditional security mechanisms like encryption have proven to be ineffective. To provide effective source privacy,propose a scheme Source Node Privacy(SNP) through Selection of Set(SOS)alongwith Lively Routing Path (LAP). The securityAnalysisbased on the proposed criteria, shows that the proposed scheme can provide excellent Source Privacy (SP). The messagewill send securely. The adversaries cannot able to identify the source node. Because of the secure algorithmthe adversaries cannot make anyinterruption to the message. The comprehensive simulation results demonstrate thatthe proposed scheme is very efficient, provide privacy and can achieve a high message delivery ratio. The proposed scheme is designed to save precious sensor energy.

------------------*****************---------------

I.INTRODUCTION

Wireless sensor networks consistof several nodes,they are large number of tiny low cost devices they also contain a sink as general purpose computing devices referred as base station. Nodes contain battery, processing unit and sensors. Base stations act as a gateway between the WSNs and other networks like access point (AP) or internet. Many security protocol designs are mainly focused on WSNrouting, while designing a routing protocol things like mobility of nodes and base station along with the way that the nodes are placed manually on specific location following some predefined network topology or randomly deployed in an area are very important, while designing a protocol number of nodes involved in the network is also a key factor.Even though therouting protocols are very important for a WSN still there are only a few protocols for source Privacy.

One of the major issues that jeopardize the successful deployment of (WSNs) is privacy. Usually WSNs will collect valuable data’s around the environment so the inappropriate use of suchdata’s that can significantly violate privacy. WSN is frequently used to collect sensitive information like buildingmonitoring, healthmonitoring, noisemonitoring and traffic monitoring. Side channels referred as Information leakage is a key issue in providing appropriate source privacy. Information’s like source location, sink locations are typical context oriented information they are mainly responsible for providing (SP). So while designing a protocol for source privacy two main features need to be focused. Untraceabilityis the inability of an adversary in tracking individual data flows back to their origins (or) destination. Unlinkability is preventing an adversary from linking the identity of the source and destination at the same time. Another key issue is multi hop routing; many routing protocols for WSN are Multihop protocols. These Multihop protocols may provide high efficiency in routing but they are vulnerable to location privacy violation. These protocols offer a lot of help for the adversary in order to achieve higher possible efficiency.The adversary can track data packets back to the source and destination over consecutive links. Signal detection techniques are used to track back data packets.Because of the limited battery power the sensor nodes rely on sink using multihop communication.So to provide effective source privacy we need to adapt to single hop communication or hop by hop communication. Propose a scheme that adapts hop by hop communication along with (SNP) source node privacy by (LRP).

The major contributions of this paper are the following:

1. To provide source privacy by developing a scheme SNP.
2. To develop a LAP routing path that do not allow adversary to do traffic analysis.
3. To provide effective selection of set by SOS scheme to maintain message integrity.
4. To provide extensive results in NS2 simulation to prove the efficiency of proposed work.

II.TERMINOLOGY AND ASSUMPTIONS

We assume there is a security server (SS) that is responsible for all operations inside a network. The various functions of SS are monitoring the security parameters in the network. However, after deployment, the sensor nodes are captured by the adversary and include false message to the network via compromised node, but still the compromised node cannot able to create a new public keys that actually accepted by the SS. so there is no possible way of affecting the networks by the adversaries.

The above assumption leads this paper to mainly consider two different attacks:

- Passive attacks. The adversary will capture the path and perform traffic analysis.
- Active attacks. The adversary will capture a node and obtain all possible information's and modify the content and include false messages that affect the network.

III.LITERATURE SURVEY

In the past two decades anonymous communication protocols that provide source location privacy are mix net. Amix net provides anonymity via packet reshuffling through a set of mix servers. These protocol rely on the statistical properties of the background traffic, they cannot provide provable anonymity. Another protocol that joins the way of mix net is DC-net. In DC-net only one user can send at a time it takes some additional bandwidth to handle collision and contention.

Flooding mechanisms are the important schemes that provide anonymity. They proposed a metric for measuring the source location privacy in the presence of a local adversary called safety period. It creates an identity that defines number of message the source sent before captured by the adversary, so it is easy for the adversary to trace the source because the first message to reach the adversary is the message on the shortest path to the source.

Probabilistic flooding is more energy efficient and provides higher level of source location privacy. Here a subset of node is involved in forwarding. Hence it makes the adversary to easily capture the source path.

Phantom flooding is the advancement of the previous protocols. Here the scheme contains two different phases. First message goes to a random node called (Phantom node).then in second phase the message is flooded by the phantom node to reach the destination. Still in this scheme if the random selected phantom node is compromised it may leads to a collapses of the entire network.

Random walk and path confusion in this scheme the flooding path was replaced by a single routing path. By provide such a single routing the safety period is improved since every message takes a different path to the Base station (BS) so the adversary will not have a steady state of flow so it is difficult for the adversary to trace back but the key issue here is battery power, for each different way the precious sensor energy is wasted. Greedy random walk provides two way random walk from both source and the base station. Random parallel routing follows a different approach where each node will take a multiple disjoint path to the base station that is pre-defined.

Secure implicit geographic forwarding (SIGF) that defines each stride is only one hop long. Follows up by geographic position of neighboring nodes.

Fake source and dummy traffic provide a main theme of hiding real data in a fake source. Do not protect against global adversary but send a dummy message or real message in predefined intervals. Real message are hidden in with dummy once and network traffic is totally independent of the monitored events.

On above all scheme providing source privacy along with saving precious sensor energy was a key factor, so to do that propose an effective selection (SOS) set followed up by a routing path (LRP) is vital.

IV.SOLUTION AND MECHANISMS

First propose a scheme that provides source privacy through appropriate selection of set ST.

Propose a scheme that can provide source node privacy without tracking back with traffic analysis.

To provide source privacy, along with consideration of less energy consumption.

The source should follow a LRP that includes both source and destination.

To prevent adversaries to get the essential details of traffic analysis by capturing the routing path, the proposed scheme consists of a SOS. Selection of set was a key factor in providing source privacy. Before a message is transmitted; the message source node selects a ST from the public key list in the Security Server. Oncean adversary finds or compromises a node he can possibly find out the previous node of the source or even the real source node but the adversary will not able to know that the selected node is a real source node is some other node. because of the wrong selection of the ST,when a source node selects a particular ST to transmit data from source to destination based on an effective LRP selection, however the adversary will not able to know the particular ST at which the actual source node creates a path to transmit the messages. Hencethese provide a clear way of PROVIDING source node privacy during communication of data. Still a hop by hop communication factor is preferred for transmission of data for secure purpose.

As an example consider a group of sensor nodes in that a source node need to transmit message ,to destination without any traffic analysis by adversary, apart from a group of nodes from the network, the SOS selection of set i.e. a particular set of nodes from the overall network, that definitely includes both source and destination. After the selection of a particular set out of entire network, propose a LRP lively routing path from the selected set ST.these ensure that selection of unwanted nodes from that ST will make the proposed scheme more efficient.

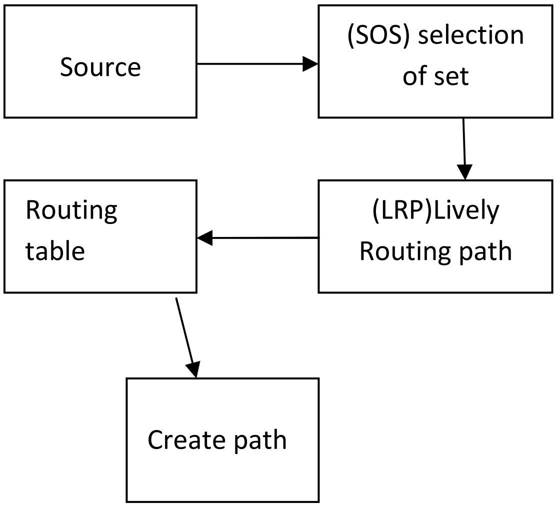


Fig: 3.1 System Architecture

V.PERFORMACE ANALYSIS

i) Select Destination:

In a group of sensor network after selection of a particular destination the entire system module changes, once clear with a destination then finding an appropriate setST become easy.

ii) SOS (Selection of Set):

Once chosen a destination finding out a particular set of nodes on the overall nodes is called SOS. These include a path that will consider only a few nodes for routing path.

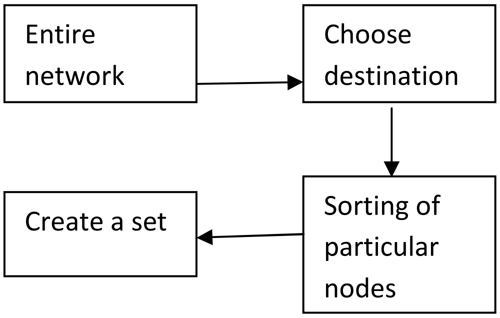


Fig: 4.1 Selection of Set

iii) LRP (Lively Routing Path)

After selection of a particular set among the entire node, based on the particular ST and destination propose a lively routing path that effectively create a path between source and destination without traffic analysis by an adversary.

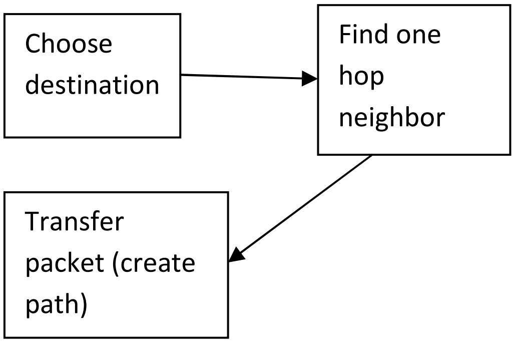
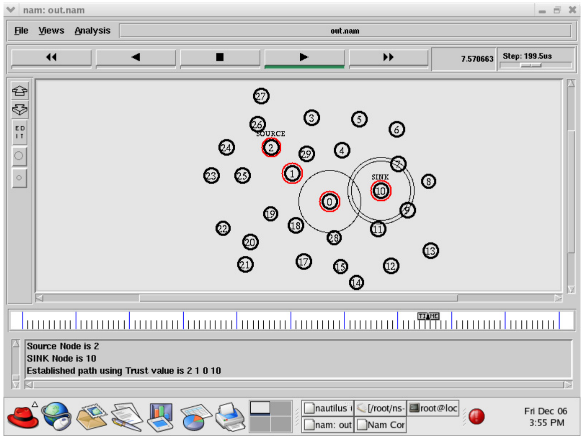


Fig: 4.2Lively routing path

VI.EXPERIMENTAL RESULTS

In this section, proposed scheme provides effective source privacy along with limited usage of energy consumption is proved by the simulation results.



Source Node is 2
SINK Node is 10
Established path using Trust value is 2 1 0 10

Fig:5.1 simulation of routing path.

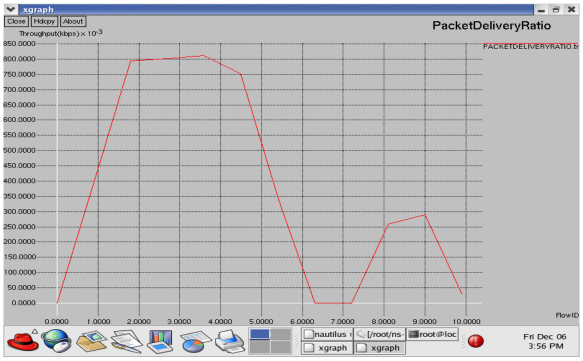


Fig:5.2 packet delivery ratio

VI.CONCLUTION

In wireless sensor networks source privacy is a key issue in effectively managing all collected data's without any security problem. Inthis paper the proposed scheme provides SNP (source node privacy). Through selection of set (SOS) andlively routing path (LRP). The proposed scheme provides provable source node privacy along with energy efficiency. Simulationresult demonstrates that the proposed scheme can achieve good performance in energy consumption and secure path creation that stopsadversary to do traffic analysis.

REFERENCE

[1] David L.Chaum,"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", ACM volume 24, 1981.

[2] Celal ozturk,Yanyong zhang, "Source Location Privacy in Energy Constrained Sensor and Network Routing", In SASN'04,pages(88-93),2004.

[3] Pandurang kamat, Yanyontg zhang, "Enhancing Source Location Privacy in Sensor Network Routing", In ICDCS'05,(pg. 599-608),2005.

[4] Yorg xi,L.Schwiebertand Weisong shi, "Preserving Source Location Privacy in Monitoring based Wireless Sensor Networks, IEEE Computer society, 2005.

[5] Jian li,Yun li,Jie Wu,"Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks",vol 25,no 5,2014.

[6] Jens Grossklags and Alessandro Acquisti. When 25 cents is too much:An Experiment on Willingness-To-Sell and Willingness-To-Protect Per-sonal Information. InSixth Workshop on the Economics of InformationSecurity (WEIS 2007), Pittsburgh, PA, USA, 2007.

[7] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking.

InMobiSys '03:Proceedings of the 1st international conference on Mobile systems, ap-plications and services, pages 31{42, New York, NY, USA, 2003. AC