International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Security for Source Node Privacy in Wireless Sensor Networks

Lavanya Ranganath[1], Kavya K S[1], Priyanka B M[1], Shruthi A M[1], Dr C VidyaRaj[2]

[1] *BE, Department of CSE, NIE Mysuru, Karnataka, India*
[2] *Professor, Department of CSE, NIE Mysuru, Karnataka, 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. The proposed system provides privacy to the tracking sensor node and integrity to the data gathered by the sensor node. Sensor Network uses random walk path to send packets. It may be difficult to trace packet and location for an adversary to detect real identity in environment. The system has been proposed to provides security from eavesdropping attack, black-hole node, misbehaving, and denial of service, compromise attack and packet spoofing. It provides source node privacy using random path approach. It optimizes packet delivery ratio, energy consumption, packet delay.*

Key Words: WSN Privacy; Location Privacy; Safety Period; static Routing; Adversary

1. INTRODUCTION

In recent years, the advancement in wireless communications has enabled the development of sensor-based networks. In comparison to the autonomous traditional networks, the WSN has become a new adopted network structure. WSN inherently based on the wireless communications, which is basically an open media. An unrestricted wireless communications are more prone to privacy and security threats than the wired one. In wireless domain, anybody equipped with a sufficient hardware can intercept and monitor the wireless network communication. An adversary may use high frequency radio transceivers to monitor the network communications from a distance. It is very likely that the source location can be easily identified by the adversary through tracing its messages

Privacy in WSN can be classified into two categories: Context privacy and Content privacy [4]. Context privacy focuses on hiding the unique identity and location of the nodes and the flow of the messages transmitted within the network. An adversary can misuse the contextual information of the nodes such as its location. While content privacy deals with providing the freshness, integrity, non-repudiation of the messages and maintain its confidentiality. It deals with the data content exchanged within the network, which can be violated through data and traffic analysis attacks.

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. 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 can be used for location of the source node. Random path model is protects the source location privacy under traffic monitoring.

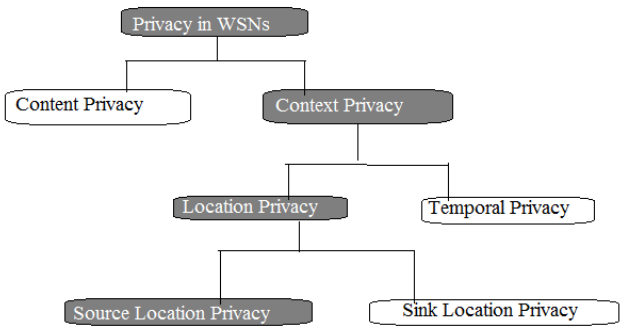

Fig 1.1 Privacy in wireless sensor networks

The proposed system is interested in tracking and monitoring application, such as tracking animal activity. Source privacy is generally compromised by Meta and contextual information on source node through packet. Adversary node can send packet at real node and try to find credential information for misuse purpose. 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.

1.1 Problem Statement

In Wireless sensor networks source node privacy is one of the important aspect. The present systems provides privacy using various techniques, such as, fake node and fake packets, flooding based techniques, privacy against traffic rate analysis. In one or the other way each technique consumes more energy in the network and increases in packet delivery delay.

1.2 Proposed System.

For source location privacy, system uses the random path to confuse the adversary. All nodes gather the information for sink node. It uses random path approach and double encryption between the communicating nodes.

2. METHODOLODY

A. Route computation module:
There are many sensors are randomly distributed in WSNs. In this system there is one base station, and many sensor nodes. Sink node or base station broadcast beacon message to sensors in communication range using UDP. Each sensors receiving beacon message will add their IP address, forward to sensors under hierarchy. All sensors creates route table containing all possible path to base station.

B. Key generation and route registration module:
In this module, each sensor generates the Symmetric Secret Key and Asymmetric Keys. Generated Public Key along with all computed routes is registered by each sensor at Base Station (Via. the shortest path). Base Station computes data encryption key (Symmetric Key) to each registering sensors. Data Encryption Keys are encrypted using Sensor Public Key. Encrypted Data and Encryption Key is given as ACK to Sensor, Further Decrypted using Private Key by sensor.

C. Data sensing and encryption module:
In this module, Content Based Privacy is provided by encrypting the Sensed data using the Data Encryption key using Symmetric Key Cryptographic Algorithm (Rijndeal Algorithm).

D. Generate shared secret key module:
The shared secret key is used for secure communication between neighbor nodes. Uses Bilinear Pairing (Diffie-Hellman Algorithm) to generate shared secret key. Data to exchange gets re-encrypted using shared secret key (Symmetric Key Cryptographic Algorithm).

E. Data forwarding module:
Source node decides random route to forward its data to base station Using Random Route Selection Algorithm (Custom Algorithm).system uses selected random route to forward data from source sensor to BS using TCP Protocol for Communication. Every forwarding sensor will re-encrypt data using shared secret key.

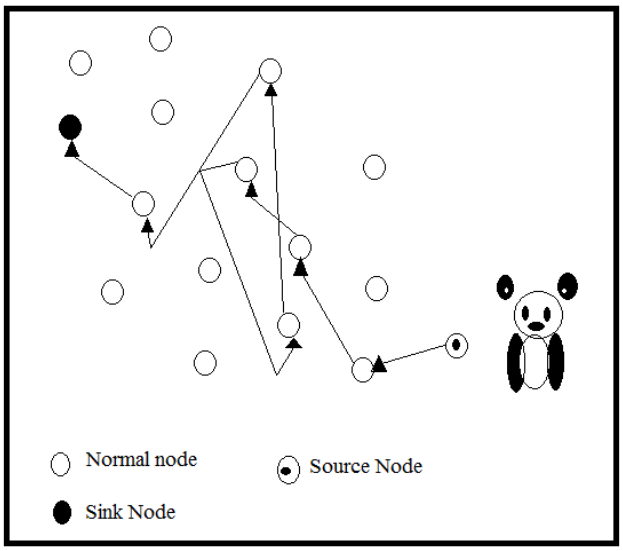

Fig 2.1 Random route selection

F. Data Decryption Module:
When the packet received by Base station, decryption is performed using the Data Encryption key of source sensor. Data Log happens at base station.

3. CONCLUSIONS

Preserving source location privacy in wireless sensor networks is a challenging issue as it can be used by various monitoring purposes as well as by the military surveillance.

Due to the openness of network architecture, an adversary can easily trace the location of the source node by using the backtracking. In this paper, system introduced a protocol that helps to minimize the network traffic and creates randomness for the message route.

REFERENCES

[1] Pradeep Kumar Roy and Rimjhim "An Efficient Privacy Preserving Protocol for Source Location Privacy in Wireless Sensor Networks" IEEE WiSPNET 2016 conference.

[2] Kangfeng ZHENG and Dongmei ZHANG "Anti-Pollution Source Location Privacy Preserving Scheme in Wireless Sensor Networks" IEEE 2016 conference.

[3] Shruti Gupta, Bhaskar Prince "Preserving Privacy of Source Location using Random walk: A Survey" IEEE International Conference -2016.

[4] Devdatt Nadre, Balaso N. Jagdale "Security for Source Node Privacy in Wireless Sensor Network" international conference-2015.