Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY

Full Length Article

Establishment of Security Threads In Wireless Sensor Network

[a] J.Rajakumari, [a] S.Poornima, [a] V.Ramya, [a] S.Saranya, [b] R . Sudhakar.

[a]*Department of Computer Science and Engineering, Nandha College Of Technology, Erode -638052, Tamilnadu, India*

[b]*Assistant Professor, Computer Science and Engineering, Nandha College Of Technology, Erode -638052, Tamilnadu, Indi*

***Corresponding Author**
R.Sudhakar
(sudhakar.r@nandhatech.org)
Tel.:9944522778

Received : 19-7-2017
Reviewed : 25-7-2017
Revised : 26-7-2017
Accepted : 05-8-2017

DOI:

ABSTRACT:

Wireless sensor network are networks in which data are obtained by observing the environment by a large number of sensors deployed in a specific area are sent securely in the network. The conducted simulation results and corresponding analysis demonstrate the proposed algorithms state of art schemes in terms of detection accuracy and effectiveness. Authentication key establishment protocols between a sensor and a security manager in a self-organizing sensor networks.WSN are vulnerable to different types of attacks such as (Sybil ,Wormhole, Sinkhole, Selective forwarding attack) low battery power and low in energy. Routing algorithm problem is one of the major issues in WSN. It compare the protocol in terms of energy consumption and network lifeline. Finally this paper present a technique to reduce the computation at sensors required by these schemes.

Keywords: Wireless Sensor Networks, Detection Accuracy, Attacks, Routing.

1 Introduction

WSN are rapidly growing due to low cost solutions for a variety of challenges in the world. Sensor are devices are working on harsh weather conditions, reduce in energy consumption ,designing low cost sensors in high capacity .Example applications include target tracking, scientific exploration and monitoring of nuclear power plants. It usually composed to a large number of nodes that work together to accomplish a sensing task. The major security for these attacks such as size of sensors, memory processing power, various expected from sensors.

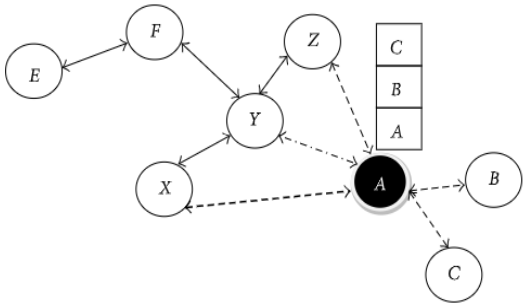
2 .A SECURITY THREADS ON NETWORK LAYER IN WSN

- Sybil attack
- Wormhole Attack
- Sinkhole Attack
- Selective Forwarding Attack

2.1 SYBIL ATTACK :

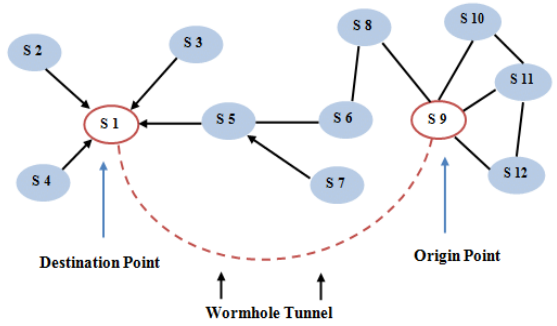
- The malicious node pretends to be multiple nodes by taking multiple identities.
- It mainly used for communicates with multiple nodes.

SYBIL ATTACK WITH MULTIPLE IDS,



2.2WORMHOLE ATTACK

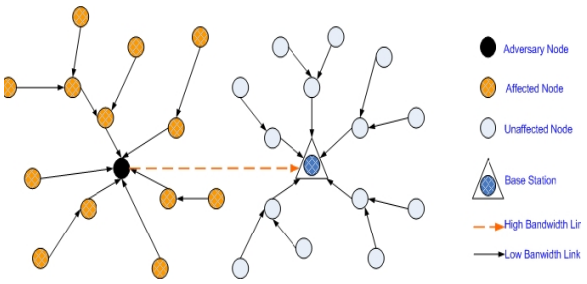
An attacker who leaks into a part of the network receives messages over a low-latency connection and can repeat them in different parts through a tunnel.



WORMHOLE ATTACK

2.3 SINKHOLE ATTACK

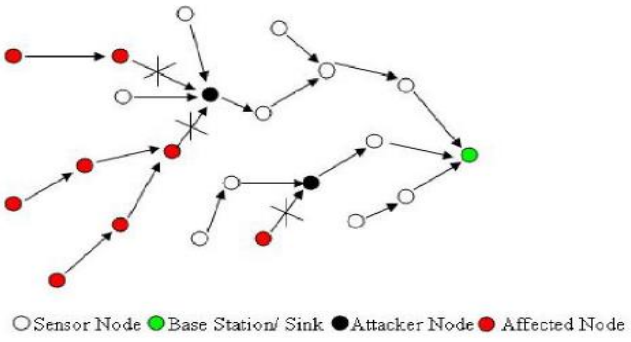
A node that leaks to the network acts like a sink node, pulling all data packets onto it. In this attack, all network traffic is in danger.



EXAMPLE OF SINKHOLE ATTACK

2.4 SELECTIVE FORWARDING ATTACK

A malicious node that has leaked to the network destroys an incoming message to transmit. This node is similar to a black hole and is used to block the flow of data.



SELECTIVE FORWARDING ATTACK

3.RELATED WORK AND PREVIOUS WORK:

3.1 RELATED WORK

The various public-key based key establishment protocols is used to set up symmetric link keys. Cross-node and node to center authentication is required because node must know each other and securely exchange the data .The main idea is sensors are randomly pick a set of keys from a key pool before deployment. The information provided directly to determines the accuracy of localization results. Detecting and isolating malicious nodes (unwanted nodes or attackers or hackers) in the network.

3.2 PREVIOUS WORK:

The various types of attacks are involved in various applications of WSN such as military application , health application, scientific application, environment applications are monitoring the security requirements such as integrity , confidentiality , authenticity, scalability in WSN. The malicious node attempt to replace the data items with unnecessary ones. After detecting the attack the malicious node messages exchange with other nodes. The major issues is node over problem and inefficient attacker detection accuracy.

4. PROPOSED WORK

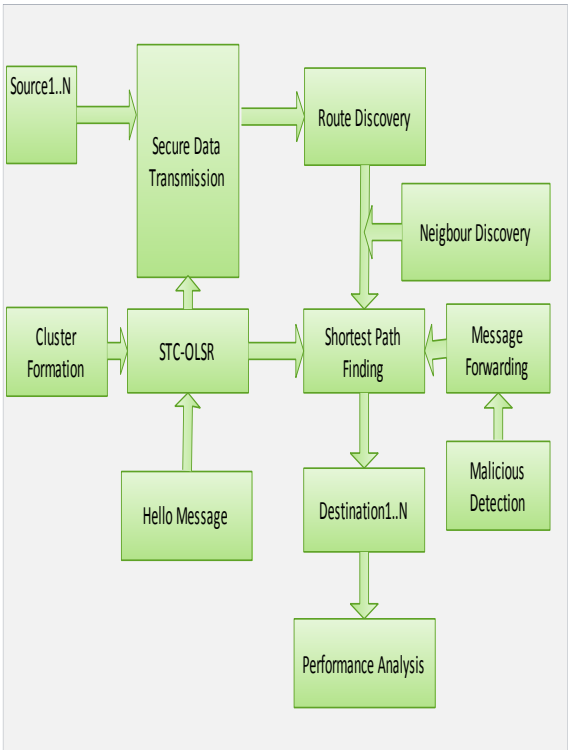
In proposed work involves source authentication, data integrity, immediate authentication, time synchronization and communication overhead. It reduced the computational overhead for key exchange in low power device with the help of a more power server. The periodically updating the symmetric keys are shared by all the sensor nodes. The network will record the identities of all other nodes it hears broadcasting after the series of time intervals. The length of observation period are mainly depends on the amount of mobility within the network. The proposed algorithm containing network assumption, communication model, attacking model and malicious node detection algorithm .The protocol of STC-OLSR is mainly used for finding the shortest path and it acquires secure trust based systems in it.

4.1 ADVANTAGES:

- Enhanced attacker detection and prevention.
- Reduced average end-to -end delay and routing overhead of messages .
- Exception handling for node overhead problem.

- High security level.

4.2 ARCHITECTURE DIAGRAM OF PROPOSED SYSTEM



5. CONCLUSION:

The develop of general framework are pool based key distribution in sensor networks .The nodes are communicate directly to establish a keys are arranged to be closed to each other. To explore the space of sensor network routing .The overall energy consumption of the nodes is reduced, leading prolonged network lifeline. This research is helpful to analysis the behavior of WSN without any attack in WSN after the deployment of WSN.

6.REFERENCES:

Copyright 2016 S.R.Rajeshwari and V. Seenivasagam" Comparative study on WSN".various authentication protocols in

Huang Q ;Cukier .J;Kobayashi.H;Liu,B;Zhang,J." Fast authentication key establishment protocols for self-organishing sensor networks".

Heena Sharma, Awaz Dhawan." An Enhanced and efficient mechanism to detect Sybil attack in WSN.

Jalil Jabari Lot Institute of Technology University of ANAS."Hierarchical routing in wireless sensor networks : a survey".

Donggang Liu cyber defence laboratory at north carolina state university."Establishing Pairwise Keys in Distributed Sensor Networks.

Aykut karakaya Internet and network technology program.Zongulang ,TURKEY." A Survey on Security And Authentication Approaches in Wireless Sensor Networks.

Xingcheng Liu,Senior Member,IEEE,Shaohua Su, Feng Han , Yitong Liu, Zhihong Pan." A Range -Based Secure Localization Algorithm For Wireless Sensor Networks".