ISSN : 2278- 9723
http://dx.doi.org/10.31838/ijccts/07.02.01

Research Article

A SECURITY THREATS AND AUTHENTICATION APPROACHES IN WIRELESS SENSOR NETWORKS

R.SUDHAKAR[1],RAJAKUMARI.J[2],POORNIMA.S[3],RAMYA.V[4]

[1234]NANDHA College Of Technology. Erode-52.Department Of Computer Science And Engineeering
Email id :sudhakarcs87@gmail.com, jrajakumari52@gmail.com,
tkpoorni9788@gmail.com,anirark9@gmail.com

Received: 01.01.19, Revised:01.02.19, Accepted: 01.03.19

ABSTRACT

Wireless sensor network are used for the replacement of wired networks and it communication is much faster compared to wired networks. 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 produces the various types of attacks such as (Sybil, Wormhole, Sinkhole, Selective forwarding attack) It uses the low battery power and low in energy. Hackers can hack the data while in sending from one system to another. The malicious detection is mainly used the protocol of (*STC-OLSR*)to find the shortest path algorithm. It compare the cost with neighbor nodes to find the least difference to delivers the packets from source to destination in it.

Keywords: Wireless Sensor Networks, Detection Accuracy, Attacks.

INTRODUCTION

WSN are rapidly growing due to low cost solutions for a variety of challenges in the world. Malicious detection are mainly used for identification of attack and using the shortest path algorithm to detect the attacks in it. The protocol of STC-OLSR (*SECURE TRUST CLUSTERING-OLSR)*is provide the secure or trust based security. Nodes misbehaves are represented in malicious node and it mainly used in fields as WAKI-TAKI is used to delivers the secure information for network hacking. The major security for these attacks such as size of sensors, memory processing power, various expected from sensors.

Security Threats On Network Layer In Wireless Sensor Networks

Sybil Attack: The single node that communicates with multiple ID's. The multiple ID's that defines the attacker node in the network.

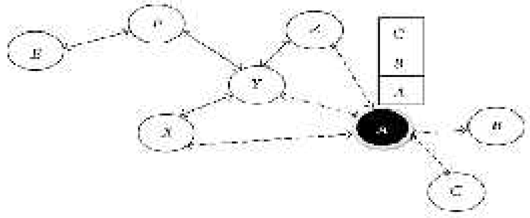

Fig.1: Sybil attack with multiple ID.

Wormhole Attack The data packet is sending from source to destination while some errors are occur to dropped the packets. This leads to delivery of packet get lost or deleted.

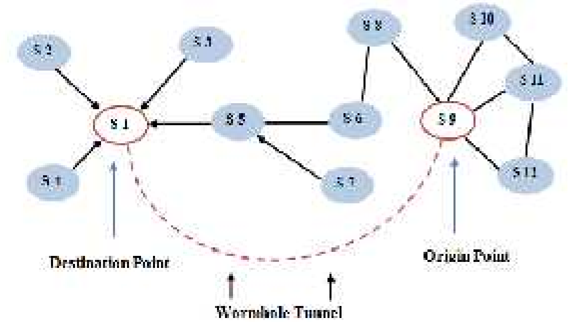

Fig.2: Packets get dropped in sending the data.

Sinkhole Attack
It redirects the traffic from destination to attract the network by using the fake ID's of routing information.

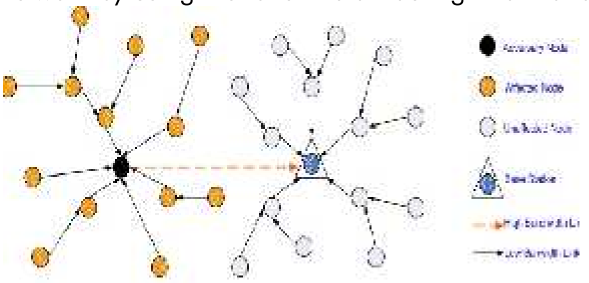

Fig.3: Redirects the unfaithful data.

Selective Forwarding Attack
The fake phone number call is turned on from base station to affect the nodes. It has multiple sensor nodes with single base station to forward the call from unknown servers.

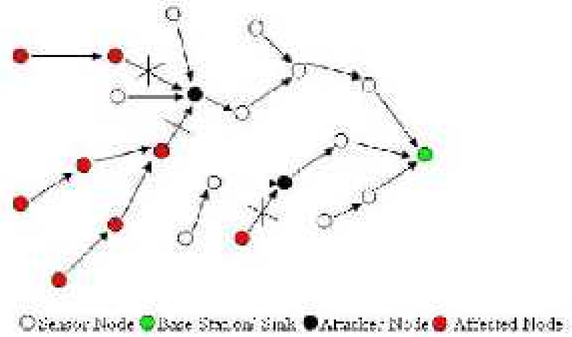
○Sensor Node ●Base Station/ Sink ●Attacker Node ●Affected Node

Fig.4: Unknown calls are forwarding the attack

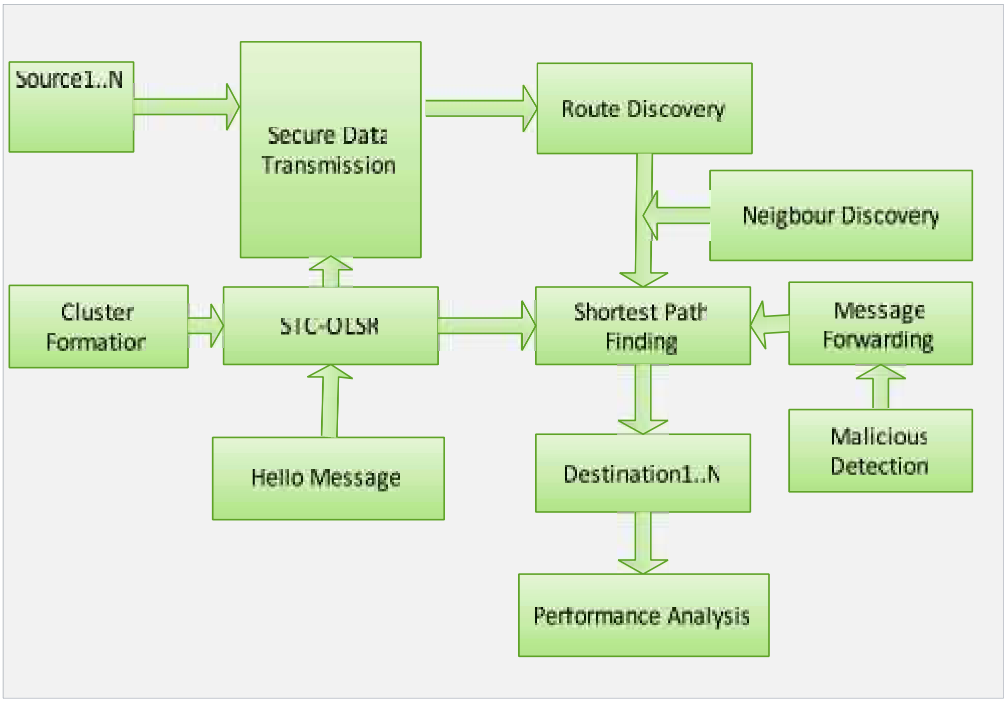

Fig. 5: Architecture diagram of proposed system.

Related Work And Previous Work

Related Work

Authentication approaches based protocol is used to establish the security through the keys .The main idea of sensors are smaller in size that communicates to detect the attacker nodes. 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. The misused detection and attacking system are mainly involved in related works.

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.

Proposed Work

In proposed work involves source authentication, data integrity, immediate authentication, time synchronization and communication overhead. The node to node overhead problem is occurs in previous work is detected in proposed. 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. The malicious node is used for the unwanted nodes are detected and the attacks are eliminated in it.

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.

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 .Using NS2(NETWORK SIMULATOR) that represents what are the security threats are present and how the threads are avoided by using the shortest path algorithm in it. This research is helpful to analysis the behavior of WSN without any attack in WSN after the deployment of WSN.

References

1. Copyright 2016 S.R.Rajeshwari and V. Seenivasagam" Comparative study on various authentication protocols in WSN".
2. Huang Q ;Cukier .J;Kobayashi.H;Liu,B;Zhang,J." Fast authentication key establishment protocols for self-organishing sensor networks".
3. Heena Sharma, Awaz Dhawan." An Enhanced and efficient mechanism to detect Sybil attack in WSN".
4. Jalil Jabari Lot Institute of Technology University of ANAS."Hierarchical routing in wireless sensor networks : a survey".
5. Donggang Liu cyber defence laboratory at north carolina state university."Establishing Pairwise Keys in Distributed Sensor Networks".
6. Aykut karakaya Internet and network technology program.Zongulang ,TURKEY." A Survey on Security And Authentication Approaches in Wireless Sensor Networks".
7. Xingcheng Liu,Senior Member,IEEE,Shaohua Su, Feng Han , Yitong Liu, Zhihong Pan." A Range -Based Secure Localization Algorithm For Wireless Sensor Networks".