International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 12, December 2014

Secured Data Transfer with Keys Management-Routing Protocol In WSN

Priyanka [#1], Er. Ankita Mittal[*2]

[#1] Student (Mtech ECE), Electronics and communication Department, Kurukshetra university, Kurukshetra, India
[*2] Assistant Professor, Electronics and communication Department, Kurukshetra university, Kurukshetra, India

***Abstract*— Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor destruction or replacement. WSNs must be secured to prevent an intruder from obstructing the delivery of correct sensor data and from forging sensor data. The focus of this paper is on routing security in WSNs. In this paper we introduce the working of distance with the collaboration of datarate enhancement in order to fasten the data transfer rate and delay reduction Most of the currently existing routing protocols for WSNs make an optimization on the limited capabilities of the nodes and the application-specific nature of the network, but do not give any importance to the security aspects of the protocols. Although these protocols have not been designed with security as a goal, it is extremely important to analyze their security properties.**

***Index Terms*—wsn, security, matlab, dsr,dsdv,routing.**

I. INTRODUCTION

Security is one of the most important aspects of any system. The communications in sensor networks applications in healthcare are mostly wireless in nature. This may result in various security threats to these systems. These threats and attacks could pose serious problems to the social life of an individual who is using the wireless sensor devices. Security requirements in WSN to ensure trustworthy and secure connections and communications are a combination of the specifications for computer network and wireless communication security. We classify the main aspects of wireless sensor network security into three major categories:

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. Public key cryptography and symmetric key cryptography is mostly used for this.In silent attacks, the attacker compromises a sensor node and feeds wrong data. Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs.

A. DoS attacks on the physical layer

Physical layer is engaged with frequency selection, carrier frequency generation, signal detection, modulation and data encryption. Jamming is the most common way of injecting DoS attack on this layer.

B. DoS attacks on the link layer

Link layer is exposed to multiplexing of data streams, data frame detection, medium access control and error control. The attacks when elevated on this layer results in collision, resource exhaustion and unfairness in allocation of frames.

C. DoS attacks on the network layer

Network layer is exposed to different types of attacks such as spoofed routing information, selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding.

D. DoS attacks on the transport layer

Transport layer is exposed to flooding attack and de-synchronization attack.

E. DoS attacks on the application layer

Application layer is exposed to logic errors and buffer overflow .

II. SECURITY REQUIREMENTS

1. Data Confidentiality

A sensor network should not leak sensor readings to its neighbors.Especially in a military application, the data stored in the sensor node may be highly sensitive. In many applications nodes communicate highly sensitive data, e.g., key distribution, therefore it is extremely important to build a secure channel in a wireless sensor network. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

2 .Data Integrity

Provision of data confidentiality stops the outflow of information, but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data

ISSN: 2278 – 909X

integrity can be provided by Message Authentication Code (MAC).

3. Data Freshness
Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design.

4. Availability
Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.Additional communication also consumes more energy. A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

5. Self-Organization
A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

III. SECURITY REQUIREMENTS

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network . The jamming of a network can come in two forms:constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently.

1.The Sybil attack
Newsome *et al.* describe the Sybil attack as it relates to wireless sensor networks . Simply put, the Sybil attack is defined as a "malicious device illegitimately taking on multiple identities. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks

2.Traffic Analysis Attacks
Wireless sensor networks are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations. It is not unusual, therefore, for data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an adversary to effectively render the network useless, the attacker can simply disable the base station.

3.Homing
In homing attack, the attacker investigates the network traffic at the network layer to interpret the geological area of cluster heads or base station adjoining nodes. It then implements some other attacks on these crucial nodes, so as to physically destroy them that further cause major destruction to the network .

4.Neglect and Greed Attack
This attack occurs at the network layer. When a packet is transmitted from a sender to a receiver, then in between both these nodes, there occur a number of other nodes through which the packet is routed before reaching to the final destination. Transmission is said to be successful when the packet is completely reached to its destination. In the meanwhile, malicious node can force multi-hopping in the network, either by splashing some packets or by routing the packets towards a wrong node. This attack disturbs the behaviour of the adjoining nodes, which may not be able to receive or send messages.

5.Homing
In homing attack, the attacker investigates the network traffic at the network layer to interpret the geological area of cluster heads or base station adjoining nodes. It then implements some other attacks on these crucial nodes, so as to physically destroy them that further cause major destruction to the network

6.Black holes
Also known as sink holes occurring at the network layer . It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighbouring nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

7.De-synchronization
De-synchronization occurs at the transport layer . This attack tries to disturb an existing connection. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence the energy of nodes is wasted, therefore degrading the performance of the whole network.

8.De-synchronization
De-synchronization occurs at the transport layer . This attack tries to disturb an existing connection. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence the energy of nodes is wasted, therefore degrading the performance of the whole network.

IV. PROBLEM FORMULATION

In wireless sensor network communication is done through node to node with the help of sensor nodes. Each node in network has a sensing capability , very limited energy supply, less power. In previous methods, data is transmitted where distance determination was necessary.

In distance based systems, energy is more utilized due to large distances. In earlier systems only distance is considered and even few on advancements on data rate enhancement are dione nobody work in field of data routing along with

ISSN: 2278 – 909X

providing data security in routing protocols the work is only done in only either on routing purpose or only on security means individual fields which leads the system to handle many problems as:-

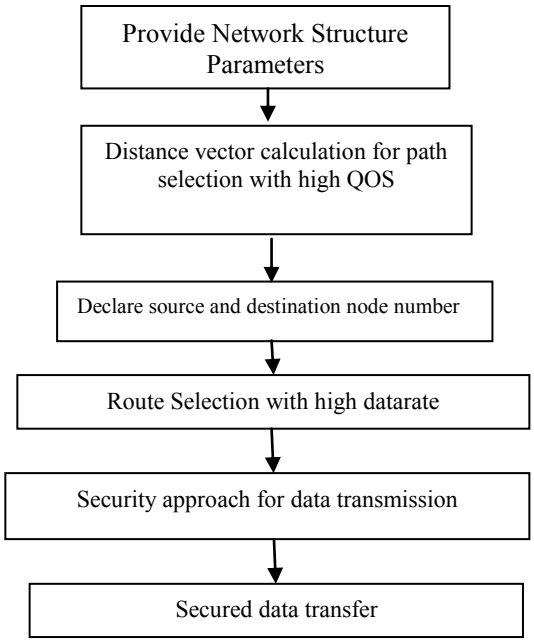
1. Attack of malicious nodes causing loss of data and interferences in data were various factors which incorrupt the transmission in Wireless sensor networks.

V.PROPOSED WORK

In this paper an approach is proposed which is solving the coming issues of routing and finding best optimal path on the basis of fast data rate along distance.
In proposed system firstly source will send the data to the node by detecting the highest datarate.
Firstly, we have to determine the distance and throughput of the nodes. Now which path has to be followed for accurate /healthy communication is detected. An acknowledgment is provided back to the transmitting node as the information regarding whether data is received properly or is lost.

Later on an approach of secure data transmission which work on basis of keys matching is given in which each node in selected route is generating individual keys up to 8 bit keys methodology. After assigning keys to each node these node match keys generated by them and do the repetition of generation up to 70% of keys get matched when the desired objective is achieved later on the transmitter node provide a dedicated key for receiver to whom it has to transfer data. This same scenario is repeated up to the data reached to destination.

VI. FLOW CHART



VII. METHODOLOGY

a. First step is to initialize all the parameters of the network such as antenna, coverage area, etc
b. Now determine total numbers of nodes and define them.
c. To find the efficient path of transmission follow as explained.
d. Next step is to determine the distances between the nodes which is performed using Distance Vector Routing algorithm in full network.
e. Among the total numbers of nodes select source and destination node.
f. Finally find the exact path of transmission with following of the proposed methodology of high datarate.
g. Later on an key allotment based approach is applied in which nodes selected in route match keys for link creation.
h. Secured data is transmitted from source to destination with fulfilling all objectives

VIII. RESULTS

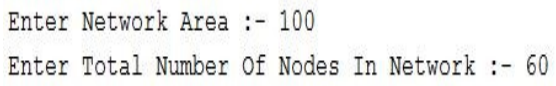


Fig 1: Structure of WSN

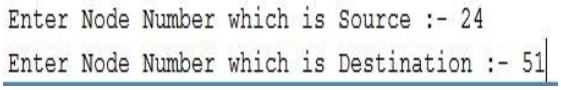


Fig 2: Defining Source And Destination Node

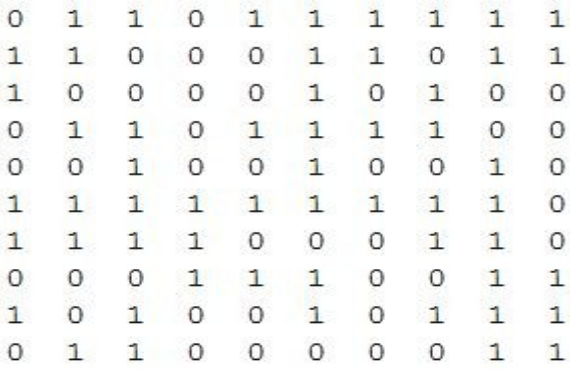


Fig 3: Key matching for Data Transmission

Fig 4: Fixed Keys Assignment

REFRENCES

[1] R.Vanilla, "Multi-level group key management technique for multicast security in manet", Journal of Theoretical and Applied Information Technology,Volume 49, issue 2, pp. 472-480,(2013)
[2] Bezawada Bruhadeshwar, "Routing Protocol Security Using Symmetric Key Based Techniques", ieee,(2010)

ISSN: 2278 – 909X

[3] Seema, Reema Goyal "A Survey on Deployment Methods in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 7,PP.540-543, (2013).
[4] Amith Khandakar "Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol", Mobile Ad hoc network is network where nodes communicate without any central administration or network infrastructure, Academic Journal Vol. 40, p36 (2012)
[5] Vibha Yadav "Localization Scheme For Three Dimensional Wireless Sensor Networks Using GPS enabled Mobile Sensor Nodes" International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1 (2009)
[6] Rajesh Sharma "Dynamic Source Routing Protocol (DSR)",The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Volume 3, Issue 7 ,(2013)
[7] Amit N. Thakare"Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks", IJCA Journal, vol 3, pp-125-128, (2010)
[8] Parul Kansal "Compression of Various Routing Protocol in Wireless Sensor Networks"have emerged as an important new area in wireless technology. International Journal of Computer Applications PP 14-19 ,Volume 5– No.11 (2010)

ISSN: 2278 – 909X