IDENTIFICATION OF MALICIOUS SENSOR NODES FOR SECURE COMMUNICATION IN WIRELESS SENSOR NETWORKS

I. Venuka Devi[1], G. Murali[2]

[1]*M. Tech, Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*
[2]*Assistant Professor of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*

Abstract

WSN (Wireless Sensor Network) has a wide range of applications.WSN are mainly used in many real world applications for monitoring the approach. AOMDV is an On-demand multipath reactive routing protocol. This protocol initiates route inventory process between sender and receiver in multiple paths, and these paths are guaranteed to be loop free. In this paper investigates the problem of minimizing the packet loss rate in the presence of malicious sensor nodes in the network. The malicious sensor nodes are identified based on energy threshold in the network. The packets are transmitted from source to the destination in malicious free path by using Hashing Technique. The nodes which are having excess energy threshold levels these nodes considered as malicious sensor nodes. Usually malicious nodes are identified based on malicious message transmissions in a network. In this paper, it forwards the data from source to destination securely with the public key and private key in Hashing Technique. The simulation result shows that this approach achieves a very low packet loss rate and high throughput with variation in data rates in the presence of malicious sensor nodes in the network.

Keywords: *Wireless Senor Network, AOMDV, Randomized Multipath Routing, Hashing Technique, Loss rate.*

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

1. INTRODUCTION

Wireless sensor network is a collection of self governing sensor nodes and one or more base stations. Each senor node sends its data observed from the physical environment to its desired base station. The sensor nodes are resource constrained. In order to save the energy constraint the power level of each sensor node is put up as low, prominent to little communication range. For this reason data gathering is performed in a multi-hop way[1] .There may be more possible routes available between two nodes over which data can be transferred. Each sensor node generates some information and this information needs to be delivered to the destination node. Every packet generated from a sensor node ought to pass to the desired base station via a routing path. If any node is long from its neighbor node then large amount of transmission energy is required to transmit the data to distance node. After completion of every transmission, remaining energy of this node decreases and some a counts of data transmission this node will be eliminated from the network because of no battery power and in this situation no node is available for data transmission and overall network lifetime will decreases.

WSN has a huge applications, including Agricultural Monitoring, Human Behavior monitoring, warfare etc [2]. Sensor nodes monitor the environmental conditions like temperature, sound, pressure etc. These rules effect classical security algorithms are unacceptable for WSNs.So new techniques in consideration of these limitations are essential.

There exist a more number of attacks an attacker can attack against wireless sensor networks, once some number of sensor nodes is convinced in a network. In the network and routing layer, the attacks include selective forwarding, sink hole, Sybil, wormholes, HELLO flood attack, black hole attack, and DDOS attacks etc. In application layer, attackers may convince sensor nodes and insert wrong data to fool data aggregators [2]. To cope with the attacks detection scheme have been investigated. These types of attacks may cause many security problems.

Among these the one is HELLO flood attack. In the HELLO flood attack attacker sends HELLO packets to sensor nodes with high radio transmission range with this the total network is isolated and is spoofed by the attacker [3].

In this paper proposed a malicious node detection scheme based on Energy Threshold and also minimizing the packet loss rate in the presence of malicious sensor nodes in the network. The nodes which are having excess energy threshold level, those nodes considered as malicious nodes. The packet loss rate is equal to the percentage of the total number of packets dropped by the base station over the total number of packets produced by all the sensor nodes.

The simulation result shows that our approach achieves a low packet loss rate by identifying the malicious sensor nodes in the network.

2. RELATED WORK

2.1 Hello Flood Attack

In Hello flood attack HELLO messages are used in many protocols by nodes that want to reveal their existence and closeness to their neighbors. Most of these protocols await on the expectation that a node *A* is within the radio

transmission range of another node *B* if *A* is able to receive messages from *B*. In a HELLO flood attack, a malicious node may try to transmit a message with an disparately high power so as to make all nodes believe that it is their neighbor[3].By receiving HELLO packets from malicious sensor node to all the nodes the total network is isolated and is ultimately spoofed by an attacker.

Proposes [4] a simple yet effective scheme to catch both packet droppers and modifiers. According to the scheme, a dynamic routing tree rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink, each packet sender or forwarder adds a small number of extra bits, is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping rate associated with every sensor node. As the tree structure dynamically changes every certain time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. The information of node behaviors has accumulated, the sink periodically run our proposed *heuristic ranking algorithms* to identify most likely bad nodes from suspiciously bad nodes. In this way, most of the bad nodes can be gradually identified with small false positive.

It is widely recognize that multipath routing is a power full solution to the HELLO Flood attack problem. Multipath routing decreases the chance of packet being dropped by a malicious sensor node by using multiple paths.

Proposes [2] a malicious and malfunctioning node detection scheme using dual-weighted trust evaluation in a hierarchical sensor network. Malicious nodes are effectively detected in the presence of natural faults and noise without sacrificing fault-free nodes. In detecting malicious nodes, we employ trust values of sensor nodes to reflect their track records in decision making process.

Proposes [3] a mechanism based on signal strength and geographical information for detecting malicious nodes staging HELLO flood attacks. The idea is to compare the signal strength of a reception with its expected value, calculated using geographical information and the pre-defined transceiver specification. A protocol for disseminating information about detection of malicious nodes is also proposed.

Proposes [5] three techniques for identifying Malicious sensor nodes. Node Monitoring, Packet sealing, Node classification. In Node Monitoring, nodes are continuously monitored for forwarding behaviors and reputation of every node is published among the network and maintained in central sink node. In packet Sealing when the sensor data are transmitted by nodes to sink, each packet sender or forwarder seals the data by adding a small number of extra bits called packet seals, from which sink could obtain useful data related to the transmission. Based on the packet seals, the sink can figure out the dropping ratio of every sensor node. In Node classification the sink identifies and classifies the nodes that are droppers.

Proposes [6] Com Sen, an intrusion detection system for identifying compromised nodes in WSNs that satisfies all these constraints Accuracy, Flexibility ,Robustness ,Scalability. Our primary goal of designing and implementing Com Sen , to improve the overall security of WSNs by providing a system for accurately identifying compromised nodes.

Proposes [7] as Stop Transmit and Listen (STL) to find the malicious node. Initially, the sensor nodes are heavily deployed over the region. Each node is having the built-in time limit to stop their transmission. Each and every node is having the capability of finding malicious node.

All the previous malicious sensor node identification approaches easy for the attackers to find the target sensor nodes for attacks. In this paper proposed energy efficient scheme to identify malicious sensor nodes, and analytically investigates the security and performance of the proposed schemes. Extensive simulations are conducted to verify the validity of the proposed schemes.

3. PROPOSED SCHEME

The target WSN is static, i.e., the region of each sensor node is immovable. There is only one base station. Each sensor node has a set of neighboring sensor nodes with which it can communicate directly. Each communication link is bidirectional. The whole network is connected, i.e., for each sensor node, there exist a routing path between this sensor node and the base station. When a sensor node produces a packet, this packet needs to be sent to the base station. No data aggregation is performed during data collection. The problem of identification of malicious sensor nodes and minimizing the packet loss rate in the existence of HELLO flood attack in a static wireless sensor network with one base station. Our objective is to identify malicious sensor nodes and also minimize packet loss rate .It is difficult for the attackers to attack the packets from target sensor nodes.

Our approach contains four major phases initialization phase, Randomized multipath routing, Identification of malicious sensor nodes, Minimizing the packet delivery failure rate. In the initialization phase we are constructing the minimum cost spanning tree with AOMDV protocol and assigns Unique ID to each sensor node. The ID of each sensor node is used in Randomized Multipath Routing. In second phase, when a sensor node originate a packet it creates three copies and forwards these three copies to the base station in different paths. In order to difficult for attackers to attack the packets chooses two paths random. In third phase identifying the malicious sensor nodes and providing security for WSN. The fourth phase is minimizing the packet loss rate.

3.1 Initialization Phase

In the initialization phase, our approach constructs a minimum cost spanning tree *T* rooted at the base station with the maximum lifetime and assigns a unique ID to each sensor node in a distributed way. Distributed naming algorithm contains two phases .In the first phase, the base station creates a message for calculation of the size of each sub tree in *T*. This message will be sent to each sensor node along the tree *T*. When it reaches to a leaf sensor node, the leaf sensor node will send an acknowledgement message to its parent in *T*. An acknowledgement message sent by a sensor node contains the size of the sub tree rooted at the sensor node. When a sensor node receives the acknowledgement messages from all its children, it calculates the size of the sub tree rooted at it self. In the second phase, the base station initiates a message for assigning a unique ID to each sensor node. This message carries the rank of the receiver of this message.

3.2 Randomized Multipath Routing

After construction of spanning tree and assigning Unique ID to each sensor node, every sensor node can start sending its originated packets to the base station.

When a sensor node originates a packet it should be delivered to the base station, it creates three copies for the same packet and sends these three copies to the base station along three paths. To make it difficult for attackers to attack the packets from some number of target sensor nodes constructs two paths at random. Specifically, when a sensor node *vi* initiate a packet, it generates two natural numbers *X* and *Y* between 1and the maximum ID of the sub trees rooted at the base station's children by using a random number generator. The first copy is sent to the base station along the path from *vi* to the base Station in *T*. The two paths for the second copy and the third copy are selected as follows.

Algorithm: Randomized multipath routing phase for the base station

==========

If a copy of a packet is received for the first time then
Set a timer for this copy;
If the timer expires then
If at least two identical copies have been received
Then
Accept any one of the identical copies;
else
Reject the packet;
end if
end if
end if

The base station accepts a packet only if it receives at least two identical copies. In this randomized multipath routing when the number of malicious sensor nodes increases packet loss rate increases.

3.3 Identification of Malicious Sensor Nodes

In our approach malicious sensor nodes are identified based on the energy threshold level of sensor nodes. Initially the energy of the sensor node is kept as 10 joules. The number of sensor nodes considered as 30.The energy threshold level of sensor nodes reaches to then these nodes considered as malicious nodes. The malicious sensor nodes are having excess energy threshold levels than normal sensor nodes.

Node Energy Model

The Node energy model is used for modeling the energy of sensor nodes. In this approach we are accurately identifying misbehaving or malicious sensor nodes by measuring energy threshold level of each sensor node in the network. Enabling or using the energy for wireless node gives accurate results.

Node energy model used in the below manner.

Set Val (rp) AOMDV
Energy model $Val (energy model)
Set Val (initial energy) 10

This energy model code will be added to the node configuration code for getting accurate results.

3.4 Minimizing the Packet Loss Rate

In our approach after identifying the malicious sensor nodes the sender generated packets are transferred to the base station in malicious free path using Hashing Technique. In order to minimize packet loss rate the sender transfers the packets to base station in secure path.

3.4.1 Hashing Technique

In Hashing Technique source node checks all of its neighbor nodes and intermediate nodes of shortest path to the destination using Hash Function Technique. Hashing is used to Encrypt and decrypt digital signatures .Digital Signature is transformed with the hash function and then both the hashed value and the signature are sent in separate transmission to receiver. With the usage of same hash function as the sender, the receiver extract a message digest from the signature and examine the message digest it obtained.

In Hashing Technique the source node originate HASH_ID using the following Hash Function.

H (n) =PUB KEY/IP ADDRESS

All the neighbor nodes to source originates HASH_ID using Hash Function H(n).The source node delivers encrypted data to the destination.

Hash Function is used to indicate the exact value or key and then used subsequently each time the data combines with the value or key is to be fetched.

4. SIMULATION RESULTS

Consider a static wireless sensor network with 30 sensor nodes. UDP is a transport layer protocol.CBR is the constant bit rate attached at the sender nodes to generate traffic. Loss Monitor is attached with receiver node; Loss monitor objects trace out the lost packets and received packets. The data rate is changed and simulation time is fixed for throughout the simulation. The simulation results show that thempacket loss rate minimized at data rates 1 and 2Mbps. Packet loss rate increases when data rate increased, shown in fig-1.

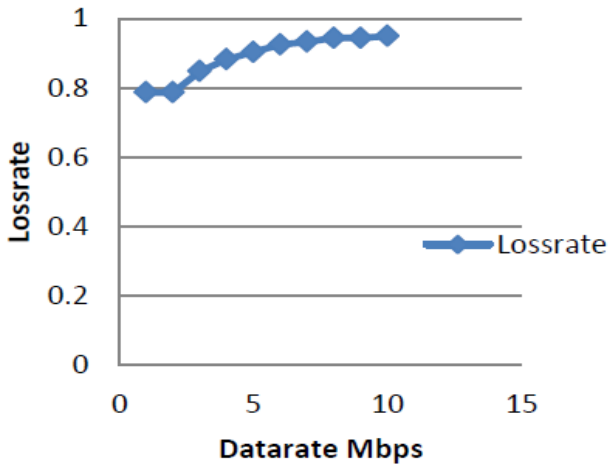

Fig- 1 Loss rate with variation in data rate

Throughput is the amount of data transmitted in a period of time. At data rates 1 to 5 Mbps AOMDV has best throughput and then it decreases shown in fig-2.

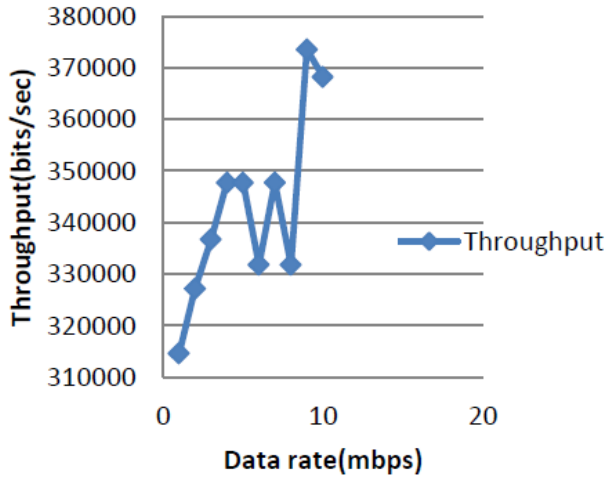

Fig-2 Throughput with variation in data rate

5. CONCLUSION

Wireless sensor network is prone to attacks easily so providing security is the main challenge. Here Hashing technique is used to improve the performance by varying data rates. By using new techniques, improves the performance and security of the network becomes a challenge in the future.

REFERENCES

[1]. Wael Y. Alghamdi, Hui Wu, Jingjing Fei, Salil S. Kanhere "Randomized multipath routing for secure data collection", IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)Symposium on Security, Privacy and Trust for Cyber-Physical Systems, Singapore, DOI 10.1109/ISSNIP .2014.6827598, April 2014.

[2]. Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi , "A malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks", Wireless sensor network, 2012 , 4, 84-90

[3]. Waldir Ribeiro Pires Junior, Thiago H.de paula Figueiredo, Hao Chi Wong, Antonio A.F. Loureiro, "Malicious Node Detection In Wireless Sensor Networks", IEEE International Conference on Advanced Information Networking and Applications, Barcelona, DOI 10.1109/WAINA.2013.135, March 2013.

[4]. Chuang Wang, Timing Feng, Jinsook Kim, Guiling Wang and Wensheng Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, DOI 10-1109/TPDS.2011.117, April 2011.

[5]. S.Sivananthan, K.KiranKumar, G.Saravanagokul, "Identifying Malicious Nodes in Wireless Sensor Networks Using Node Classification", International Journal Of Innovative Research in Computer and CommunicationEngineering,ISSN:23209798,November 2013.

[6]. Yi-Tao Wang, Rajive Bagrodia, "ComSen: a Detection system For Identifying Compromised Nodes in Wireless Sensor Networks", Sixth International Conference on Emerging Security Information, Systems and Technologies, ISBN: 978-1-61208-209-7, 2012.

[7]. T.SathyaMoorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini, "A Simple And Effective Scheme To Find Malicious Node In Wireless Sensor Network", International Journal Of Research in Engineering and Technology, ISSN: 2319-1163, Vol:03, Feb 2014.