NODAL TRUST ACQUISITION AND FISH BONE ROUTING IN WIRELESS SENSOR NETWORKS

[1]S.Sruthi,[2] J.Ahalya Mary, [3]L.Pushparani

[1]PG Scholar,CSE Department,SRM University,Chennai

[2]Asst.Professor in CSE Department,SRM University,Chennai

[3]PG Scholar,CSE Department,SRM University,Chennai

Email: [1] ssruthi93@yahoo.co.in

[2]Ahalyamaryj@gmail.com

[3]pushpakokila@gmail.com

***Abstract*—Wireless sensor networks play a promising role in wide range of applications such as remote tracking and environment monitoring. Wireless Sensor Networks (WSN's) are prone to various security attacks. Black hole attack is a classification of attack that affects data gathering. Acquiring nodal trust helps mitigate black hole attacks (BLA). It works by launching detection routes to detect intruder's location and behavior. The information obtained using the detection routes are useful in avoiding malicious nodes being chosen for data transmission. Nodal trust scheme in combination with fishbone routing avoids black hole attacks and prevents data leakage. While the nodal trust scheme is confined to identifying malicious nodes, fishbone algorithm identifies the shortest path for data transmission. A node with high trust and located nearby to the sink node is chosen for data transmission by the fishbone algorithm. Trust calculations are based on the delivery ratio of data flowing through the chosen node. If a node is found to drop packets its trust is set to a lower threshold value and is not selected for data forwarding. Nodal trust scheme along with fish bone algorithm can significantly increase the data route success probability, ability to withstand black hole attacks and can optimize network lifetime.**

Keywords—Wireless sensor networks, Black hole attacks, nodal trust

I. INTRODUCTION

Wireless Sensor Network (WSN) has emerged as one of the prominent technologies, since they are potentially low cost solutions to a variety of real-world challenges. Wireless sensor networks are sometimes referred to as wireless sensor and actuator networks. These networks are spatially distributed autonomous sensors used to monitor environmental and physical parameters such as sound, PH level, temperature, etc.

A WSN is typically composed of a large number of low-cost sensor nodes which work collectively to carry out some real-time sensing and monitoring tasks within a designated area. Realization of a WSN faces many challenges. Although some of the wireless adhoc networking techniques are applicable to WSNs, they differ from a mobile adhoc network(MANET) in many aspects. Typically, sensor nodes are more resource constrained in terms of power, computational capabilities and memory [2].All the sensor nodes are usually designed to sense its local environment and send data of interest back to base station which is several magnitudes more powerful than sensor nodes and acts as concentration point of the WSN to rest of the world.

Reliable data delivery has been a major concern in WSNs since nodes are suspicious to failure and interferences. Long transmission paths and self-congestion due to collision and radio interference make reliable data delivery in WSN a challenging phenomenon. Security is another major concern in sensor nodes. Nodes in WSNs are often unattended due to economic constraints and are subjected to various security attacks. Several general-purpose sensor network techniques assumed that all nodes are cooperative and trustworthy. This is not the case for most real- world sensor network based applications, which requires certain degree of trust to maintain proper network functionality. Therefore, developing a trust model has become the area of research in addition to the use of cryptographic functions [3].

Black hole attack is one major security threat in WSN that affects data transmission and security. Black hole attack (BLA) also known as packet drop attack is a type of denial of service attack in which a router that is supposed to forward packets instead discards them. Black hole attacks can be categorized into single black hole attack and collaborative black hole attack.

In a single black hole attack, a single node misleads the route discovery process. In the following figure, node 1 represents source node and node 4 represents the destination node. Node 3 is a malicious node which replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore, node 1 erroneously concludes route discovery process with completion, and starts to send data packets to node 3. A malicious node probably drops all the incoming packets. This suspicious node causes black hole problem. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

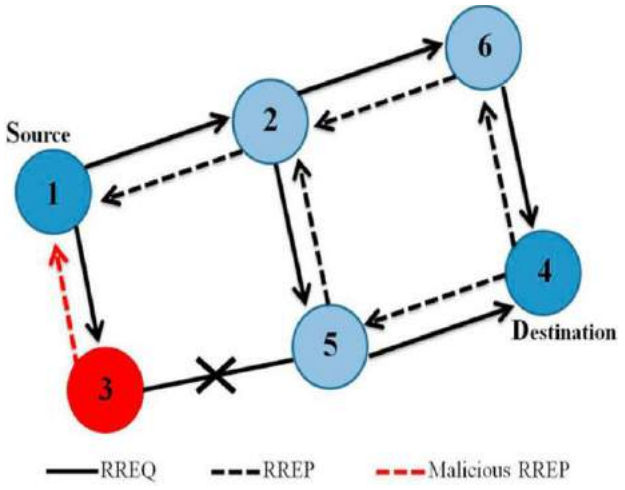

Fig 1.1 Single Black Hole Problem

Several malicious nodes might collaborate together and mislead the route discovery process which is termed as collaborative black hole attacks.

II. Literature Survey

Securing WSN is a challenging task because of its characteristics such as unreliable wireless communication, resource constraints, and unknown topology prior to deployment, physical tampering of nodes due to unattended and unprotected environment. To secure them security goals are to be satisfied. These security goals are classified into primary and secondary goals. The primary goals include data confidentiality, integrity, availability and authenticity. The secondary goals are self-organization; time synchronization and data freshness [4,10,11].WSN are easily prone to security attacks due to its deployment in hostile environment. Several security solutions of traditional networks are not applicable to WSN due to its open space deployment and resource constraints of memory and energy.

In recent years, several data routing protocols have been proposed for WSNs to ensure successful data delivery to sink node. Single-path routing protocols are simple and less secure. Several multipath routing protocols then came into existence to combat issues of single path routing protocols. The advantage of multipath routing protocols is, data can safely reach the sink, despite of attack in some route. Multipath routing protocols are classified into two based on whether the packet is split into several messages or not. They are multipath routing with share division and without share division [1].

In Non-share based multipath routing, a packet is routed via several paths to ensure data delivery to sink even if one route is compromised by intruder. Issues with such protocols is that if the packet is routed via m routes simultaneously, the energy consumption will be m times higher than single path routing, thus affecting the network lifetime. Share based multipath routing protocols split a secret message into multiple shares, these shares are delivered to sink by multiple independent paths. The advantage of such protocols is intruder should capture several shares to restore nodal information. The limitation of such algorithms is that they are deterministic. This paves way for several attacks if the algorithm is known [5,11].

To overcome issues with above routing protocols randomized multi-path routing algorithm has come into existence [6]. This algorithm computes multiple paths in a randomized way each time an information packet needs to be sent, such that routes taken by shares of various packets differ over time. In effect, a large number of routes can be generated for each source-destination pair. In order to intercept the message, adversary has to jam all possible routes and stands highly difficult. In addition to random propagation, three similar strategies namely, direct random propagation, non-repetitive random propagation and multicast tree assisted random propagation are defined [1,8].

Security and Energy efficient Disjoint Route (SEDR) scheme is proposed to route sliced shares to the sink with randomized disjoint multiple routes by utilizing the available surplus energy of sensor nodes.

To improve transmission reliability in WSN packet-loss avoidance approach and packet-loss recovery approaches have been established. In packet loss avoidance approach, the goal is to choose highly productive paths that can significantly reduce packet loss. Node selection criteria differ in various algorithms. In GeRaf the geographic distance is used as a evaluation metric for node selection [7,9].

In packet-loss recovery approaches, retransmissions are carried out to recover packet loss. Recovery mechanisms are of two type's end-to-end and per-hop recovery. End-to-End recovery mechanisms like TCP adopted in traditional networks are not applicable for wireless networks as the latency and cost involved in implementing such recovery schemes in WSN's are huge and unacceptable. Per-hop recovery such as PSFQ can be applied to WSN's. It's assumed loss-free wireless links can be provided by unrestricted per-hop retransmissions. However, in practice an unlimited number of retransmissions are prohibitive due to the large energy cost and the potential congestion. Wireless links are not los free therefore errors will accumulate and arrive at an unacceptable level for end-to-end transmission. Therefore, transmission services solely relying on per-hop recovery usually have no guaranteed service quality.

Another method to avoid attacks and ensure successful data delivery is through trust routing. Trust management is an advanced mechanism for choosing highly trusted nodes for data routing. Sec-CBSN algorithm develops different trust calculation methods to identify trusted nodes. ReTrust is an attack-resistant and lightweight trust management protocol which can resist attacks through a trust management approach for medical sensor networks.

A. Problem statement

In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi hop transmission to deliver the packet to a base station. Hence a packet is forwarded through many intermediate nodes to reach the sink.

Sensor networks are usually deployed in hostile environment where an adversary compromises some internal nods which may launch various attacks. One kind of attack caused by malicious node is black hole attack where the nod drops all the packets. Black hole attack is difficult to detect since the wireless communications are not reliable where normally there is a packet loss due to noise.

In some cases sensor nodes goes into sleep state to save power, in that period of time node cannot receive/ send data packets. Therefore it is important to identify if a packet loss is due to black hole attack or due to other reason. In order to ensure successful data delivery to sink, it is essential to identify nodes with high trust.

Calculation of nodal trust plays a critical role in successful data delivery and extensive analysis is required for the same. In addition, if the trusted node is compromised by the intruder, there should be a mechanism to identify alternate node with high trust to route the data packets to sink node.

III. Analysis of Framework

Nodal Trust is an extension made to Active Trust scheme. Active trust scheme helps in identifying the black holes and chooses nodes of high trust for data transmission. It lacks to address the fact that, a trusted node which was successful in delivering data packets in previous transmissions can be compromised by the intruder at any point in time. It doesn't provide a mechanism to overcome the issues caused by trusted node failure.

The Nodal trust scheme helps to identify the compromised nodes by establishing a detection route. Detection route refers to a route without data packets. The purpose of establishing detection routes is to convince the adversary to launch an attack so the attack behavior and black hole location can be identified [1].

Once the detection route identifies the black holes, actual data transmission process takes place through nodes with high trust. However, during further transmission, it is possible that the trusted node becomes compromised by the intruder. Therefore, it is essential to identify alternate nodes of high trust value and is located nearby sink node. The alternate nodes can be identified by using fish bone algorithm in an efficient manner.

The proposed system works as follows

- A detection route is established and dummy data packets are transmitted. When the intruder launches an attack, the location of black holes is detected.
- Once black holes are identified, actual data transmission takes place by avoiding the nodes which are found suspicious using detection routing.
- Data routing uses shortest route protocols. A node x will choose the neighbor that is nearer to sink and as high trust. If there is no such high trust nodes found, the node x will report it to the upper node. The upper node will reselect a different node from its neighbor in the same manner.
- During detection routing and data routing each node perform a trust calculation to avoid black holes. If a node is found malicious in the latest detection, then its trust should be below threshold value Θ.
- If a malicious node is found to return to normal mode, several detections are to be made to involve the node in further data transmission.
- If a trusted node which had high threshold value is compromised by the intruder and is found to drop packets, Fish bone algorithm is used to identify alternate node that is nearer to sink and is of high trust value to transmit data.

Nodal Trust Calculation:

Nodal trust can be evaluated using several methods; all the algorithms are common in terms of assigning more weight to the latest behavior. Several methods for evaluating nodal trust are defined below.

Nodal recommendation trust: Node A is the trust evaluator, node C is the target of evaluation, and node B is a recommender of A. Consider C^B_A to be the direction trust of A to B and C^C_B to be the direction trust of B to C; then, the recommendation trust of A to C is

$$R^C_A = C^B_A \times C^C_B.$$

For the trust of multiple recommendations, the calculation of the recommendation trust from A to B, B to C, etc., until D to E is

$$R^E_A = C^B_A \times C^C_B \times C^D_C \times C^E_D.$$

Comprehensive trust: Comprehensive trust is the total trust, which merges the recommendation trust and direction trust:

The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates the direction trust for each received feedback packet. Through interactions, the node obtains the recommendation trust from its neighbors and it then calculates the merged trust, for the multiple-recommendation trust. Finally, it calculates the comprehensive trust according to the below equation.

$$C^T_{A,B} = \delta C^B_A + (1-\delta)\, U^B_A$$

Fish Bone Algorithm:

Fish bone routing algorithm is used to find alternate routing nodes when the trusted node is found suspicious during further data transmission.

It involves the following calculations to identify the angle at which the alternate node can be identified.

dx = x2-x1.

dy = y2-y1.

Angle = Atan (dy,dx) *180/PI;

Where x1,x2,y1,y2 are x and y positions of the nodes.

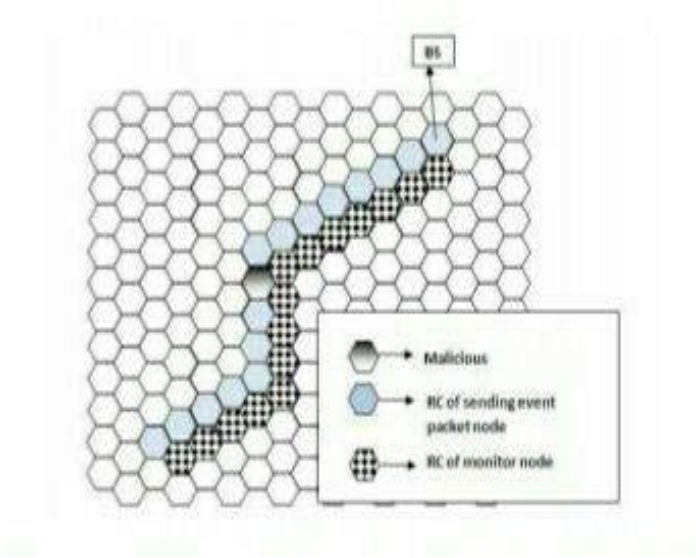

Fig 1.2: **An example where monitor node detects an attack and then reroute the packet**.

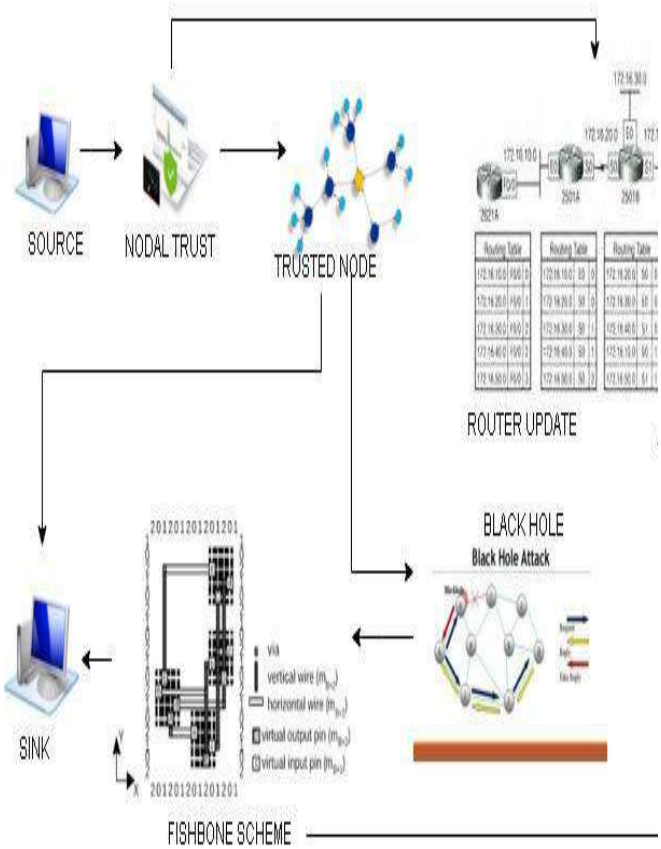

Fig 1.3 System Architecture

Algorithm

```
Initialization
For each node that receives data packet, Do
  Calculate Nodal Trust
  If ( IsPacketDelivered) Then
  Threshold >Θ
 Else
  Threshold <Θ
End-For
Update Routing Table
End
```

IV. EXPECTED OUTCOME

The performance is analyzed by using the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The parameters used for the simulation of the scheme are tabulated in Table-1.

The simulation of the proposed scheme has 60 nodes deployed in the simulation area 1000×600. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). All the nodes receive the signal from all direction by using the Omni directional antenna. During simulation time the events are traced by using the trace files. The performance of the network is monitored by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like number of packets received, number of packets lost, last packet received time etc. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay, throughput and residual energy.

Table-1. Simulation parameters.

PARAMETER	VALUE
Channel Type	Wireless Channel
Simulation Time	50 ms
Number of nodes	60
MAC type	802.11
Antenna Model	Omni Antenna
Simulation Area	1000×600
Transmission range	250m

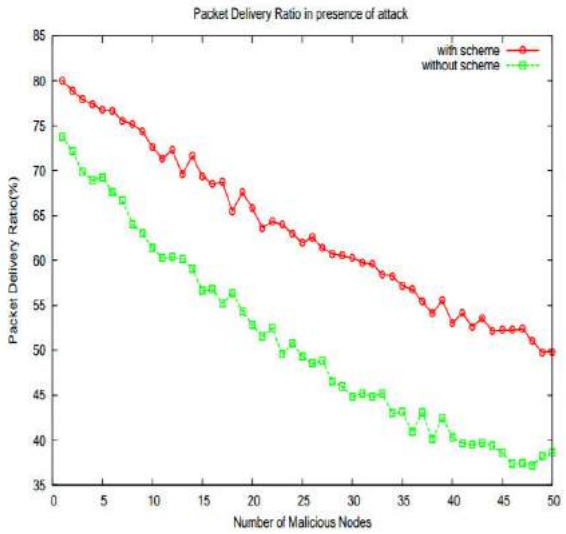

Fig 1.4. Packet Delivery ratio in presence of attack.

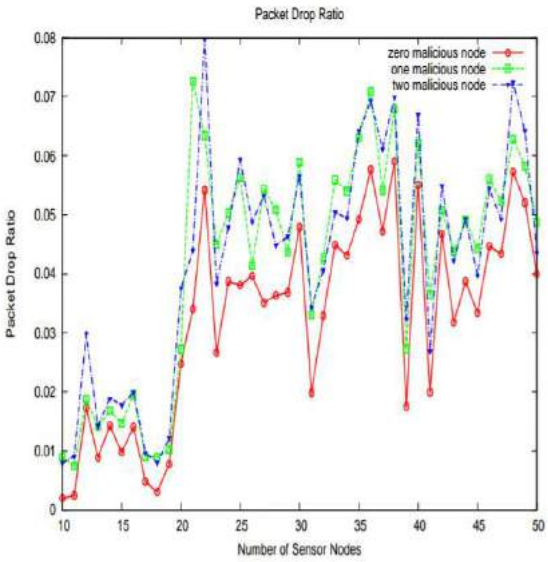

Fig 1.5. Packet Drop Ratio

Conclusion

Motivated by future sensor network applications, we studied the efficient way of identifying black hole attacks and routing the packets through trusted nodes. The Nodal trust scheme along with fish bone routing algorithm helps in successful delivery of data packets to sink node. Various data routing protocols can be used for data transmission between nodes in the proposed system.

The key concept lies in the fact that obtaining nodal trust helps to choose a node with higher probability in delivering the data to the sink. This effectively overcomes black hole attacks. Even if the trusted node is compromised at certain point during data transmission, fishbone algorithm helps identify alternate node of high trust and located nearby sink node to help in data propagation. Using various level of simulation, we can prove that the packet delivery ratio has increased despite of presence of malicious nodes, with the above approach.

References

[1] Yuxin Liu, Mianxiong Dong Kaoru Ota, Anfeng Liu,"ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Trasactions on Information Forensics and Security.

[2] W.Lou,Y.Kwon,"H-Spread:AHybridMultipath Scheme forSecure andReliableDataCollectioninWirelessSensorNetworks," IEEE Transactiononvehiculartechnology,vol.55,no.4,pp.1320-1330, 2006.

[3] John Paul Walters, Ahengqiang Liang,Weisong Shi,Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in distributed grid and pervasive computing.

[4] M.Y.Hsieh,Y.M.Huang,H.C. Chao,"Adaptivesecuritydesignwith maliciousnodedetectionincluster-basedsensor networks,"Computer Communications,vol.30,no.1,pp.2385-2400,2007.

[5] T.Shu,M.Krunz,S.Liu,"Securedatacollectioninwirelesssensor networksusingrandomizeddispersiveroutes,"IEEETransactions on MobileComputing,vol.9,no.7,pp.941-954,2010.

[6] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 12, no. 12, pp. 1091-1103, 2012.

[7] M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

[8] C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

[9] G. X. Zhan, W. S. Shi, J. L. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, 2012.

[10] D. He, C. Chen, S. Chan, J. Bu, A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions onInformation Technology in Biomedicine,vol.16,no.4,pp.623-632,2012.

[11] S.Mandala,k.Jenni,M.A.Ngadi,etal."Quantifying the severity of black hole attack in wireless mobile adhoc networks." Security in Computing and Communications. SpringerBerlin Heidelberg, 2014:57-67.