An Efficient and Reliable Approach for Wormhole Attack Detection and Prevention in Wireless Sensor Network

[1]Sadhana Devmorari, [2]Gayatri S Pandi(Jain)
[1]*Student, Computer Department, LJIET (GTU), Gujarat, India.*
[2]*Asst. Prof., Computer Department, LJIET (GTU), Gujarat, India.*

ABSTRACT

Wireless Sensor networks are comprised of many small and resource constrained sensor nodes that are deployed in an environment for many applications which require unattended, long-term operations. They are vulnerable to many kinds of attacks because of no specific network topology. Wormhole attack is one of the severe attack used to destabilize or disable wireless sensor networks. The idea behind this attack, is two or more colluding attackers record packets at one location, and tunnel them to another location for a replay at that remote location. This makes the tunnelled packet arrive either sooner or with a lesser number of the hopes compared to the packets transmitted over normal multi hop routes. Routing mechanisms which rely on the knowledge about distance between nodes can get confuse because wormhole nodes fake a route that is shorter than the original one within the network. In paper we work on trust mechanism and digital signature for detect and prevent wormhole attack . trust metrics used to address attack by monitoring behaviour of network and digital signature use for checking authentication of selected path. Through experimental results, this approach proved the network efficiency in term of improve packet delivery ratio ,end-to-end delay and throughput.

Keywords:*Wireless Sensor Network,Wormhole Attack ,Digital Signature, Trust Model*

1. INTRODUCTION

1.1 Wireless Sensor Network

A Sensor device is a small device that is able to sense environmental data(sound, light, temperature, etc.). it is also able to communicate with any other sensor node in its communication range and compute the sensed/received data. A set of these sensor devices deployed in a given area constitutes a network with no pre established architecture, so called Wireless Sensor Network (WSN). WSN hundreds or thousands of nodes are usually deployed in a large area where they can sense the environment, compute and communicate the collected data in a very efficient and distributed way.[1]

1.2 Attacks in WSN

Wireless sensor networks are susceptible to wide range of security attacks due to the multi-hop nature of the transmission medium. Also, wireless sensor networks have an additional vulnerability because nodes are generally deployed in a hostile or unprotected environment. Although there is no standard layered architecture of the communication protocol for wireless sensor network, hence there is need to summarize the possible attacks [4].

Table-1. Layering based attacks and possible Security approaches[4]

Layer	Attack	Security approaches
Physical Layer	*Denial of Service* *Tampering*	*Priority Messages* *Tamper Proofing* *Hiding,Encryption*
Data Link Layer	*Jamming* *Collision* *Traffic manipulation*	*Use Error Correcting Codes* *Use spread spectrum techniques*
Network Layer	*Sybil attack* *Wormhole Attack* *Sinkhole* *Flooding*	*Authentication* *Authorization* *Identity certificates*
Transport Layer	*Resynchronization* *Packet injection Attack*	*Packet Authentication*
Application Layer	*Aggregation Based Attack* *Attack on reliability*	*Cryptographic approach*

1.3 Wormhole Attack

In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and due to this reason this attack is serious[3].

We can use 4 steps to explain about a general wormhole attack. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes. The attacker records packets at one location of a network. The attacker then tunnels the recorded packets to a different location. The attacker re-transmits those packets back into the network location[3].

Wormhole attacks include four common attack modes: wormhole attacks usingpacket encapsulation, wormhole attacks using special tunnel mode, wormhole attacksusing high-energy transmission, and wormhole attacks using relay mode. Among them,wormhole attacks using packet encapsulation does not require special hardware performanceand not need decrypt the communication between normal nodes. Therefore, itis not only very easy to deploy, but also easy to cause greater harm[8].

Packet Encapsulation: It is a type of wormhole attack where a malicious node at one part of the network overhears the RREQ packet. It is then tunnel through a low latency link with thehelp of normal node, to the second colluding malicious nodeat a distance near to the destination node. Once this packet isreceived by the second malicious code, the legitimate neighbourof the node drops any further legitimate requests fromlegitimate neighbour node[10].

This result to the routes betweenthe source and the destination go through the wormhole link,because it has broadcast itself has the fastest route. It preventslegitimate nodes from discovering legitimate paths more thantwo hops away.For example, in Fig. 1 where A and B finds the shortest pathbetween them for packet transmission, where two maliciousnodes X and Y is present. Node A will broadcast a RREQbut because a wormhole node is present X gets this route requestand encapsulates it into the packets destined for Y, andit transmit this packet through a wormhole link tunnel. Whenthis packet is received by Y, it unmarshals the packet and rebroadcast.B being the nearest neighbour to Y will receive thispacket thinking it has come from a legitimate path. Due tothe encapsulation, the hop count will not increase during thetraversal through U-V-W-Z. Now Node B has two routes tochoose from, either A-C-D-E or A-X-Y. obeying the rules ofrouting protocols that uses metric of shortest path to choose aroute path. B will choose the shortest route path which happensto be a wormhole link. which is about 4 hops. And apparently,the wormhole link is 3 hops away while in reality is about 7hops away[10].

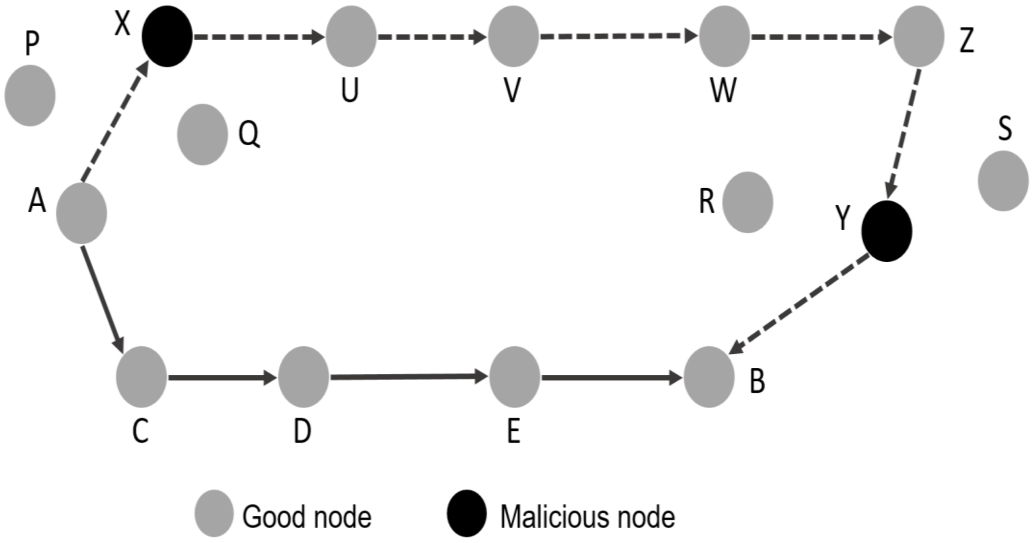

Fig. 1. Wormhole Attack using packet encapsulation[10]

2.RELATED WORK

Infrastructure less and self-governing nature of WSN is challenging issue in terms of security. Wormhole attack is one of the severe attack in wireless sensor network. based on Round Trip Time(RTT) of every route to calculate threshold RTT. According to simulation results of various parameters like Average end to end delay, Packet delivery fraction and Average throughput it is proved that proposed mechanism performs better than wormhole affected AOMDV[5].

In high power transmission mode we can gauge the transmission force of every node in the system, by utilizing the adjusted AODV convention. To finding the transmission force of every node we include the new quality that measures the quantity of transmission of node in the AODV convention. In this propose work additionally give the realness and classification on the grounds that authentic node of the system can likewise play out the powerful transmission. To separate the genuine and wormhole node that give the validness and the transmission ought to be secure by accomplishing the privacy [6].

Trust based (TAODV) protocol evaluate the neighbor nodes trust. The results show the better performance of propose scheme in terms of packet delivery, end-to-end delay and number of nodes to destination. The scheme reduced overall network delay and enhance the performance of network in the presence of different number of malicious nodes , To detect and prevent the network from these wormhole attacks, propose an enhance version of AODV hello packets. In this method assumes some assumption to apply propose method such as the clock time is synchronized and used during neighbor discovery. Neighbor nodes respond with appending Hello message with present received time and reply [7].

At the same time, the defense strategy based on monitoring neighbor node and the defense strategy based on node location information are designed and implemented. By analyzing the running. process of wireless sensor networks before and after applying these two defensive strategies, and further comparing with the running process of wireless sensor networks under wormhole attack, the actual effect of these two defensive strategies are evaluated[8].

tabu-list-based multi-path routing protocol for WSN. This protocol guarantee that multiple copies of events are delivered through completely different paths, without requiring additional communications to exchange path information. Experimental results indicated the proposed scheme which combines two tabu-lists can improve the delivery rate with a small overhead of hops and simple location-based approach. Assuming that every node knows location information of the sink and its adjacent nodes, the proposed approach tries to detect malicious nodes which fakes their hop level, as suspicious nodes. [9].

3.PROPOSED SYSTEM

The flowchart of the proposed system is as shown in Fig. 2. First InAODV routing protocol the sender node checks in the route table whether a route is present or not forcommunication of any two nodes, All the paths are stored in the routing table at sourcenode. In this way the routes are established.When source node broadcasts a RREQ packet note time t1and RREP packet receive by source and then note time t2 .using t1 and t2 value calculate the round trip time of established route.

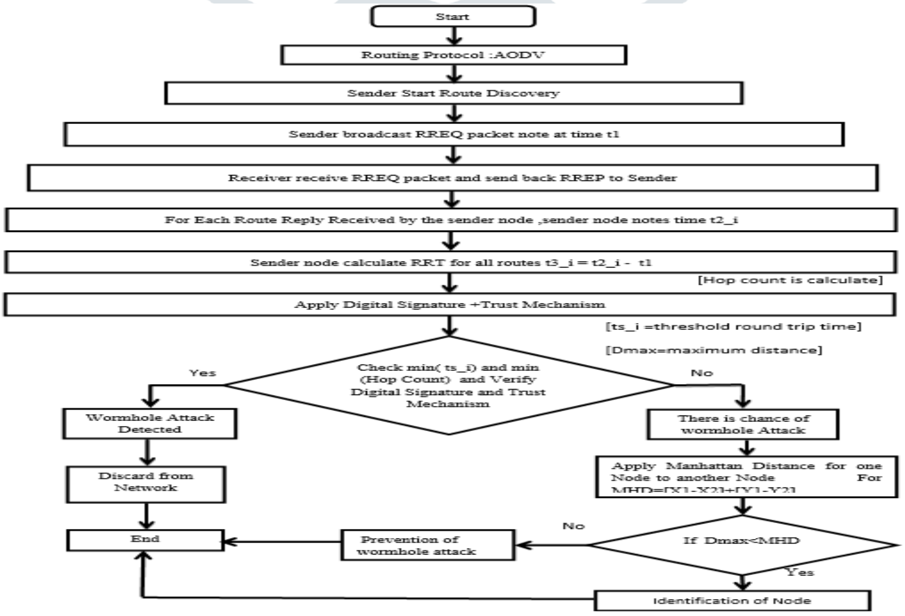
Start
Routing Protocol :AODV
Sender Start Route Discovery
Sender broadcast RREQ packet note at time t1
Receiver receive RREQ packet and send back RREP to Sender
For Each Route Reply Received by the sender node ,sender node notes time t2_i
Sender node calculate RRT for all routes t3_i = t2_i - t1
[Hop count is calculate]
Apply Digital Signature +Trust Mechanism
[ts_i =threshold round trip time]
[Dmax=maximum distance]
Check min(ts_i) and min (Hop Count) and Verify Digital Signature and Trust Mechanism
Yes
No
Wormhole Attack Detected
There is chance of wormhole Attack
Discard from Network
Apply Manhattan Distance for one Node to another Node For MHD=[X1-X2]+[Y1-Y2]
End
Prevention of wormhole attack
No
If Dmax<MHD
Yes
Identification of Node

Fig. 2.Proposed system flowchart

Overview of Proposed Method

The proposed method is more efficient and reliable for wormhole attack detection and prevention in wireless sensor network .

1. When sender broadcast route request packet it will note timet1.
2. For each route reply received by the sender node,sender node timet2_i.
3. Sender node calculates the round trip time for all routes usingformula t3_i=t2_i –t1.
4. Calculate the threshold round trip time by usingformula t3_i/hopecount =ts_i
5. Apply Digital Signature +Trust Mechanism With EachNode
6. Check the threshold round trip time and hop count is less than actual time and verify Digital Signature and Trust Mechanism With EachNode
7. If truethen
8. Wormhole attackdetected
    a. And Discard fromnetwork
    b. Else There is chance of wormholeAttack
9. So apply Apply Manhattan Distance for one Node to anotherNode

   Formula=[X1-X2]+[Y1-Y2] For further Prevention of wormhole and for broadcast safe communication.

4.SIMULATION ENVIROMENT ANDRESULT ANALYSIS

In this section the simulation results are shown for parameters like delivery rate, average end to end delay and average throughput of the packets at destination . described parameters for 10, 25, 35 and 45 nodes respectively. The wireless sensor network environment is formed using network simulator- 2.35. The following table indicates the simulation parameters

Parameter	***Value***
Simulation area	*500m X 500*
Routing protocol	*AODV*
Wireless protocol	*IEEE 802.11p*
Channel bitrate	*11Mbps*
Number of node	*10,25,35,45*
Range of transmission	*230m*
Simulation time	*200s*
Mobility model	*Dynamic*

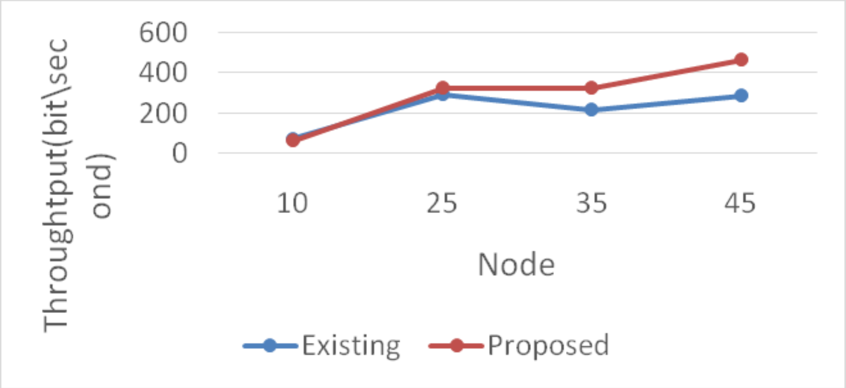

Fig . 3.Average throughput for 10,25,35 and 45 different set of node

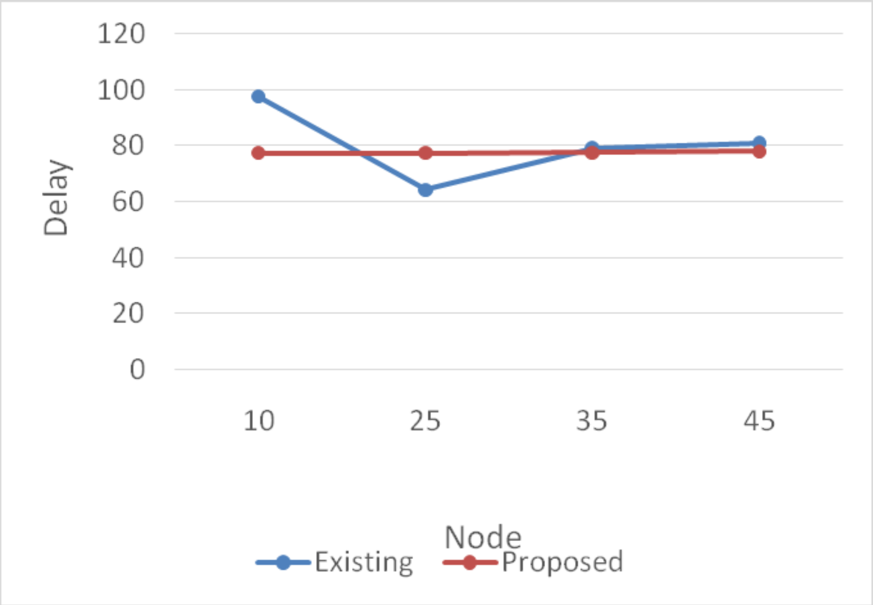

Fig . 4.Average end to end delay for 10,25,35 and 45 different set of node

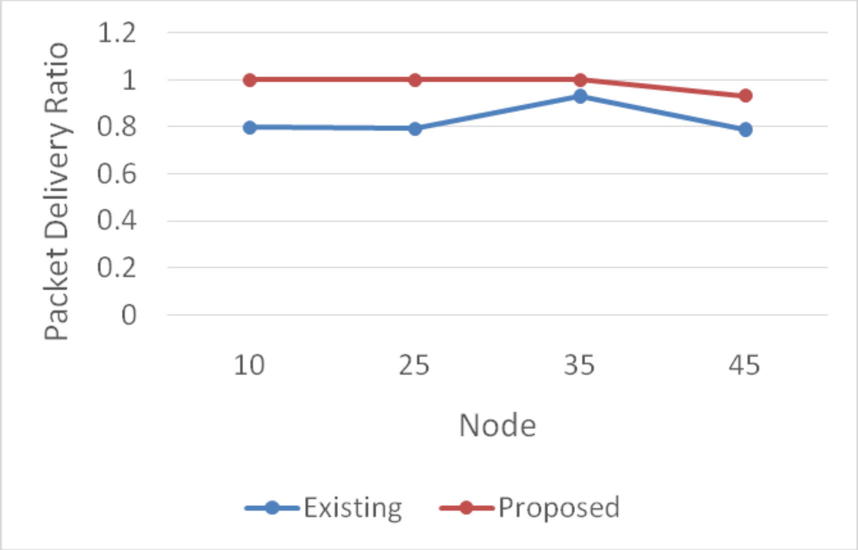

Fig . 5.Packet delivery for 10,25,35 and 45 different set of node

5. CONCLUSION

One of a kind attributes like constrained data transmission restricted battery power and dynamic topology makes Wireless Sensor Network (WSN) vulnerable to many kinds of attacks , to protect sensor network from routing attack in presence of malicious node is always challenge.Wormhole attack in WSN can be used to exploit routingcommunication in network through an adversary tunnelsmessages received in one part of the network and replays themin a different part.The experimental result show the better performance of performance scheme in term of packet delivery, end-to-end delay and number of nodes to destination. In this schemeto detection and prevention of wormhole attack weuse different method like Round trip time , Digital signature , Trust based model .

6. REFERENCES

[1] Foreword by Luigi Vincenzo Mancini In Secure Wireless Sensor Networks Threats and Solutions.

[2] George S. Oreku ,Tamara PazynyukIn Security in Wireless Sensor NetworksSpringer.

[3] Haritima Shrivastava “A Survey on Wormhole Attack Detection in Wireless Network” International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, pp.1273-1276

[4] PriyaMaidamwar,NekitaChavhan “A Survey On Security Issues To Detect Wormhole Attack In Wireless Sensor Network ,International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012”.

[5] Parmar Amisha ,V.B.Vaghelab” Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol” 2016,Elsevier pp700-707.

[6] Swati Bhagat , TrishnaPanse“A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network”2016 IEEE

[7] Raja Waseem Anwar, Majid Bakhtiari, AnazidaZainal.“Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks”2015IEEEpp56-59.

[8] Rui Ma1, Siyu Chen1, Ke Ma2(&), Changzhen Hu1, and Xiajing Wang1“ Defenses Against Wormhole Attacks in Wireless Sensor Networks”IEEE,2016.pp.413-426.

[9] Masayuki Arai “Reliability Improvement of Multi-Path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance”Spinger,2015.pp.533-536.

[10] Marcus Okunlola Johnson,Arish Siddiqui,Amin Karami “A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks”International Journal of Computer Applications,2017, pp.1-8.

[11] Ayaz Hassan Moon*a*,∗, UmmerIqbal*a*and G. Mohiuddin Bhat*b*“Mutual Entity Authentication Protocol Based on ECDSA for WSN” 2016Elsevier pp187-192.