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 ,Information Technology, L.J.I.E.T, Gujarat, India
[2] Assistant Professor, Computer engineering, L.J.I.E.T, 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 these paper we work on trust mechanism for detect and prevent wormhole attack .

Keyword : *WSN ; wormhole attack;*

---

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]

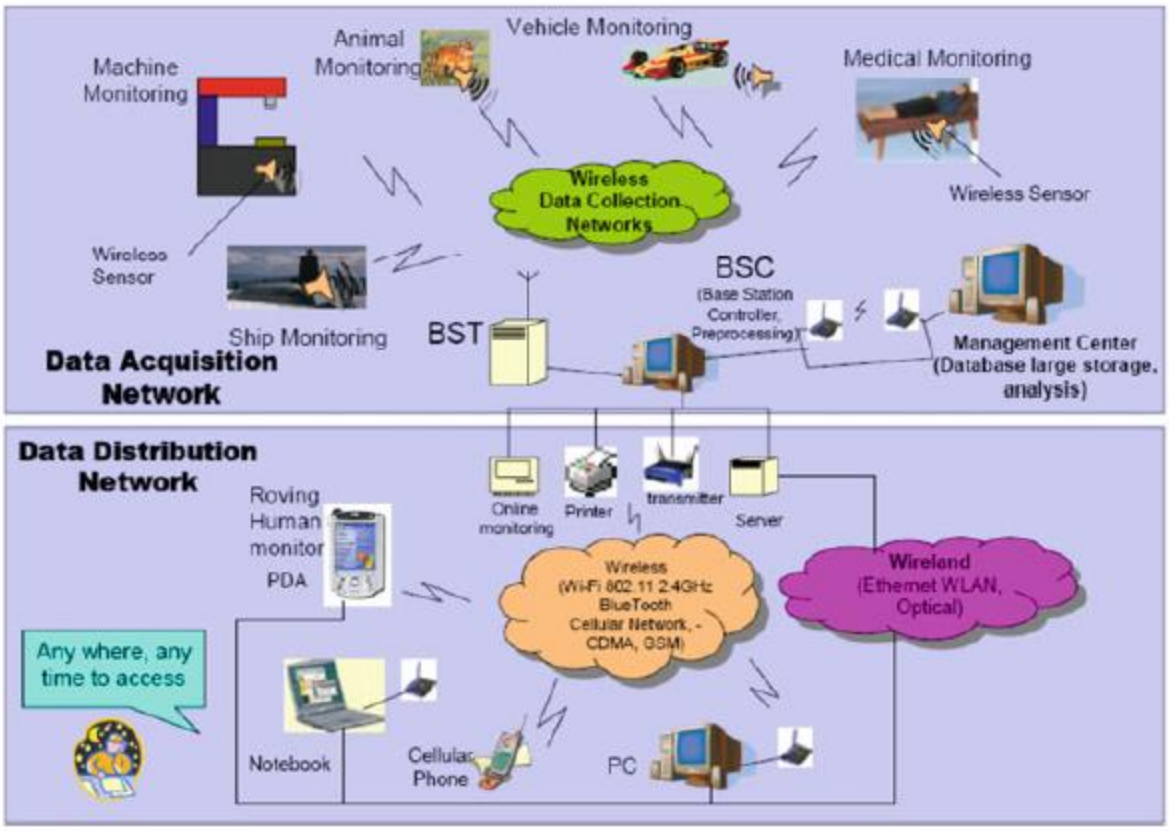


Fig -1: Wireless Sensor Network[1]

Figure 1 shows the complexity of WSNs, which generally consist of a data acquisition network and a data distribution network, monitored and controlled by a management center. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing a lot of both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a WSN. The unreliable communication channel and unattended operation make the security defenses even harder.[1]

1.2 ATTACKS IN WIRELESS SENSOR NETWORK

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	Attacks	**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 attacks Attacks 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 from as shown in figure2 [3].

Figure 2 shows the simple worm hole in the network. Here node 2 and node 8 create the tunnel in order to work as a malicious node. Both nodes give the illusion to another node that there is a shortest path. But this shortest path does not exist and attack can easily perform by the attacker[3].

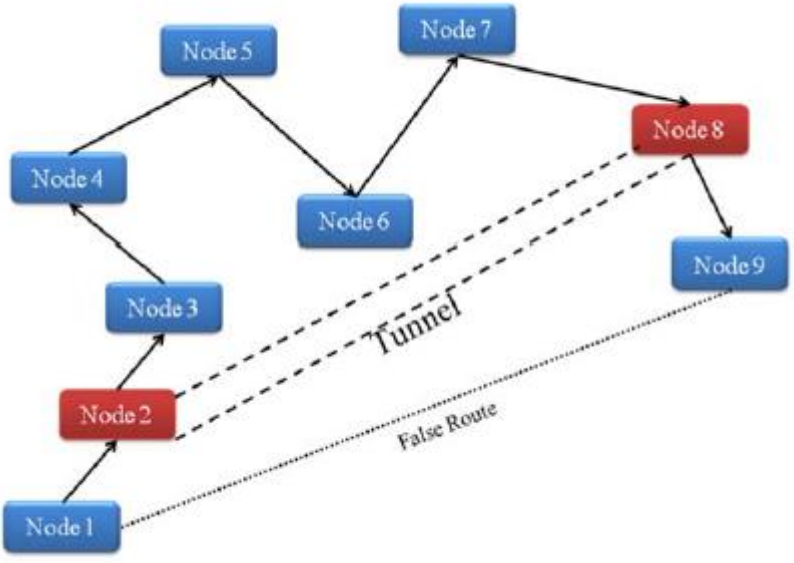


Fig . 2 Wormhole Attack[3]

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 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 massage 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].

2.1 LITERATURE REVIEW

Parmar Amish ,V.B.Vaghela [5] proposes the techniques dealing with wormhole attack in WSN are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack.

Swati Bhagat , Trishna Panse [6] scrutinize work distinguish the wormhole by their powerful transmission of the node in the system furthermore put off the system from the wormhole by accomplishing privacy in modified AODV.

Raja Waseem Anwar, Majid Bakhtiari [7] propose a trust aware distance vector routing protocol (T-AODV) to protect wireless sensor network from wormhole attacks. Through experimental results, this propose approach proved the network efficiency in terms of improved packet delivery ratio, end-to-end delay and number of node to the destination.

Changzhen Hu[8] propose the defense strategy based on monitoring neighbor node and the defense strategy based on node location information respectively. By analyzing the specific defense effect, the simulation results highlight the effectiveness of the proposed defense strategy.

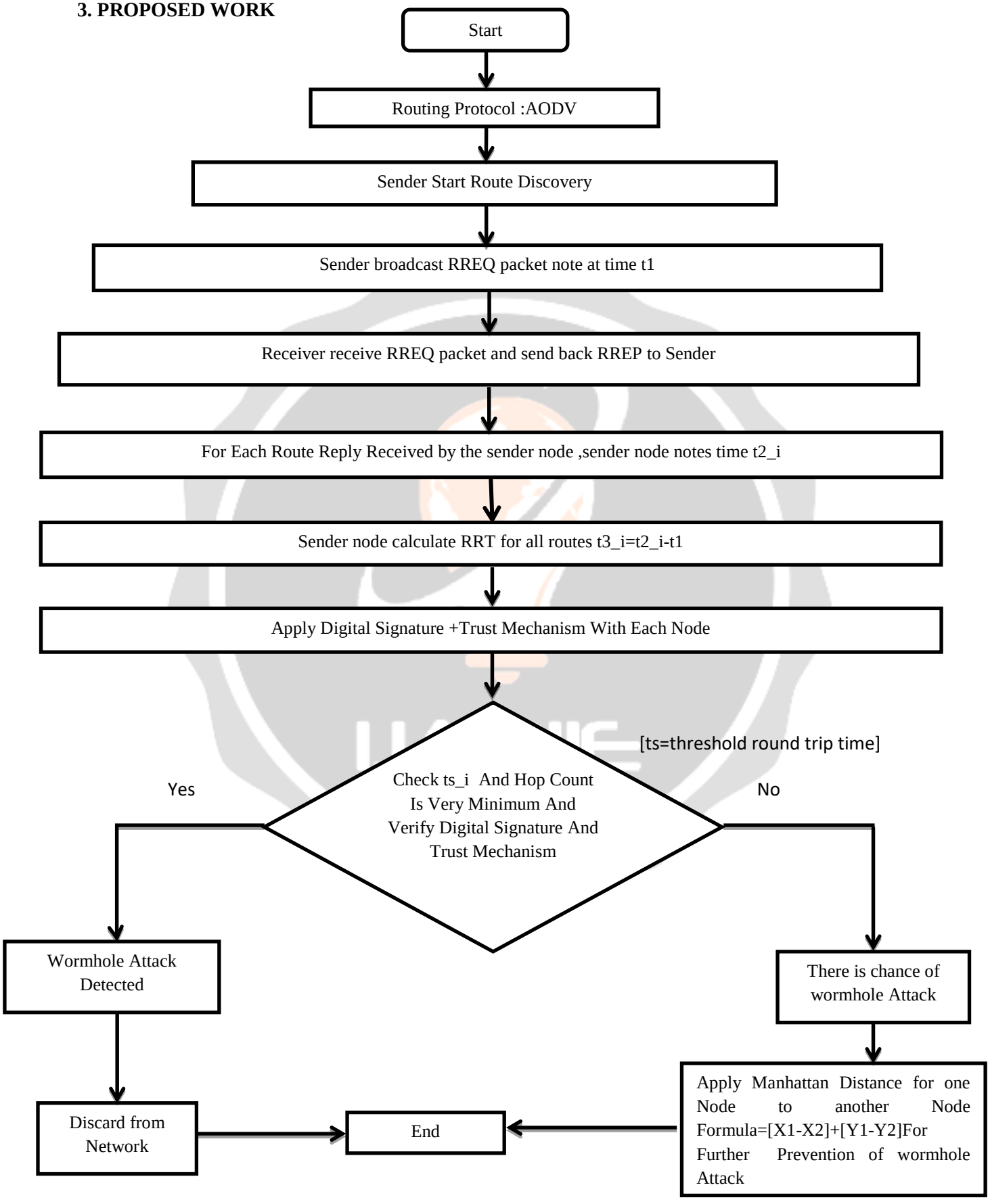
Masayuki Arai [9] propose tabu-list-based multi-path routing which guarantees that multiple copies of events are delivered through completely different paths, without requiring additional communications to exchange path information. Toward development of attack-tolerant multipath routing, we also investigate the effects of wormhole attacks and location-aware wormhole detection scheme.

2.2 COMPARATIVE TABLE

Table -2: Comparative Table

Sr.No	**Paper Title**	**Method Used**	**Advantage**	**Disadvantage**
1	Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol	RTT(Round trip time)	AOMDV protocol in our proposed mechanism is that, it has less overhead and end to end delay.	this method can not be implemented in mobile ad hoc network
2	A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network	MAODV(Modify AODV)protocol	guarantees secure routing & ensures minimum amount of idle time .	Wormhole node are false courses That are shorter than the first course in the system it makes issue indirecting component, which depend on the actualities about separation between node.
3	Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks	Trust Based	The scheme reduced overall network delay and enhance the performance of network in the presence of different number of malicious nodes.	Reliable data gathering and delivery is always a challenging task due to dynamic, unattended and unpredictable behavior of wireless sensor network and its broadcast nature of communication
4	Defenses Against Wormhole Attacks in Wireless Sensor Networks	Neighbor Node Monitoring	achieve effective defense against wormhole attacks using packet encapsulation	the shortest route strategy to judge the routing is vulnerable to the wormhole attack.
5	Reliability Improvement of Multi-Path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance	Location Based Approach	guarantee that multiple copies of events are delivered through completely different paths	This implies in dense network it might be difficult to detect malicious nodes only by location information.

3. PROPOSED WORK



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 time t1.
2. For each route reply received by the sender node,sender node time t2_i.
3. Sender node calculates the round trip time for all routes using formula

   t3_i=t2_i – t1.
4. Calculate the threshold round trip time by using formula

   t3_i/hopecount = ts_i
5. Apply Digital Signature +Trust Mechanism With Each Node
6. Check the threshold round trip time and hop count is less than actual time and verify Digital Signature and Trust Mechanism With Each Node
7. If true then
   a) Wormhole attack detected
   b) And Discard from network
8. Else There is chance of wormhole Attack
9. So apply Apply Manhattan Distance for one Node to another Node

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

4. CONCLUSION

Unique characteristics like limited bandwidth, limited 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. This paper To detection and prevention of wormhole attack we use different method like Round trip time , modify AODV , Trust based model , Location based approach , Neighbor node monitoring, and improve 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.

5. REFERENCES

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

[2] George S. Oreku ,Tamara Pazynyuk “Security in Wireless Sensor Networks”Springer.

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

[4] Priya Maidamwar,Nekita Chavhan "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 , Trishna Panse"A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network"2016 IEEE .

[7] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal."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,pp.413-426(2017)

[9] Masayuki Arai "Reliability Improvement of Multi-Path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance"Spinger,pp533-536(2015).