A Novel Approach to Detect and Prevent Wormhole Attack in Wireless Sensor Network

Rahul Patidar
Computer Science and Engineering
TRUBA College of Engineering and Technology, Indore

Ritu Tandon
Computer Science and Engineering
TRUBA College of Engineering and Technology, Indore

ABSTRACT
In our previous study [1] we discussed about Wireless Sensor Network (WSN) and also about wormhole attacks, those are possible in wireless sensor network. In this presented work the previously performed work is extended to find an optimum solution for the wormhole link prevention in the wireless sensor network. The proposed technique discover alternative route to the target node. Because the shortest path can has the malicious attacker. The implementation of the secure route discovery protocol is performed using NS2 and by modification of the AODV routing protocol. Finally the performance of the protocol is measured in terms of throughput. That demonstrates the effectiveness of the presented routing protocol.

Keywords
Wireless Sensor Network, Security, Wormhole, AODV.

1. INTRODUCTION
Wireless sensor networks are autonomous systems consisting of tiny sensors that are equipped with integrated sensing, general-purpose computing and limited-range transceiving capabilities. Due to their ad-hoc deployment sensor nodes require mutual coordination and cooperation to route information within network. Each node acts as a router for packets, which means that every intermediate node has full access to packets flowing through it. These factors make sensor networks potentially vulnerable to several different types of malicious attacks.

In the wormhole attack [4,5], a malicious node tunnels messages received in one part of network over a low latency link and replays them in a different part. Due to nature of wireless transmission, it is possible that attacker can create a wormhole, even for packets not related to it, since it can hear accidentally or secretly them in wireless transmission and tunnel them to colluding attacker at opposite end of the wormhole. The tunnel can be established in many various ways, like through an out-of band hidden channel (e. g., a wired link), high powered transmission or packet encapsulation. The tunnel creates the illusion that two end points are very close to each other, by making the tunneled packets arrive either sooner or with lesser number of hops compared to packets sent over normal routes. This makes possible an attacker to undermine (or corrupt) the correct operation of the routing protocol, by controlling numerous routes in the network. Later, attacker can use this to analyze the traffic or selectively drop data traffic. The wormhole attack mainly consists in network layer attacks when attack is classified according to network protocol stacks. A. A. Pirzada and C. McDonald [6] analyzed the creation of the wormhole.

2. VARIANTS OF WORMHOLE
There are some variants of wormhole attack will discuss here.

2.1 Sinkhole Attack
In a sinkhole attack, the goal of an adversary is to lure nearly all the traffic from a particular area through an agreed node, creating a symbolic sinkhole with the adversary at the center. Since nodes on, or near, the path that packets follow has many opportunities to tamper with application data, sinkhole attacks can empower so many other attacks. Sinkhole attacks mostly work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm [7].

Figure 1 explains how malicious node redirects with modified route sequence numbers. Here malicious node sends the sequence number which is greater than the original sequence number to misguide that it is a fresh route. Figure 2 depicts how malicious node redirects with modified hop count. Here malicious node sends lesser hop count value to tell that this is the shortest path. But, fact is that there is no such path exists. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, M absorbs all the data. So the attacks can be achieved.

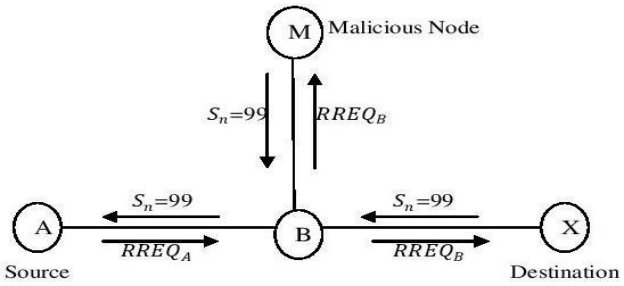

Fig. 1 Sinkhole attack with modified sequence number

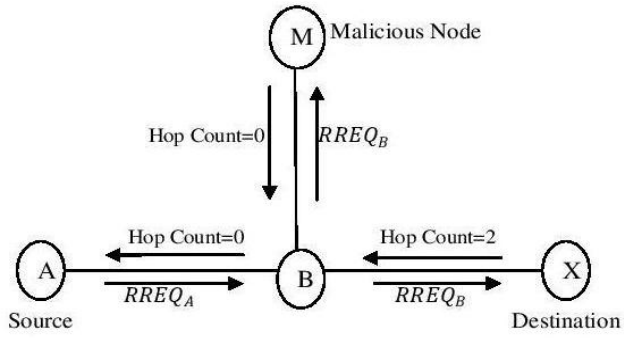

Fig. 2 Sinkhole attack with modified hop count value

2.2 Denial of Service based Wormhole Attack

Wormhole attacks can be a form of denial of service (DOS) attack [8]. The aim of this attack is to prevent legitimate Route Request (RREQ) from reaching destination. If a node needs to discover a route to a given destination, it broadcasts a RREQ packet. A high powered ("laptop-class") attacker can exploit this by tunneling each RREQ packet directly to a partner malicious node near the destination node. The partner node then broadcasts the RREQ to all its neighbors. When the destination node's neighbors hear this packet, they will follow the normal operation of routing protocol by re-broadcasting that copy of RREQ, and dropping all subsequent RREQ packets that are received for the same route discovery. This dropping of RREQ packets is an essential part of the AODV protocol to avoid redundant broadcasts. This attack thus prevents a legitimate RREQ from reaching the destination through a genuine path. The request will reach to the destination, but the intermediate nodes will not have the reverse route to the source of the RREQ, so it cannot forward the Route Reply (RREP).

2.3 Energy Depleting Wormhole Attack (EDWA)

The motive of this attack is to reduce network lifetime. An attacker achieves this by placing a single malicious node A having laptop class capability near source S. The attacker does not require another malicious node to be present in network as the recipient of the tunneled RREQ message can be any legitimate node near the destination. The attacker exploits the fact that each node only processes the first RREQ instance it receives, and ignores later instances of the same RREQ. If a node S wants the route to reach the destination D, first of all it broadcasts an RREQ to all its neighbors. The malicious node A will hear this broadcast and tunnel the RREQ to an ordinary node V near the destination using a directional antenna or high-powered transmission. When the ordinary node hears this RREQ, it further broadcasts the RREQ to its neighbors. When the destination D receives RREQ, it sends a RREP packet for the original source node S. When the ordinary node V receives the RREP, it does not have reverse route to source S, so it discards that RREP packet. Nodes near destination will drop legitimate RREQ as they already have seen this packet as a result of tunneling. Consequently, legitimate RREQ does not reach the destination [9].

2.4 Indirect Black Hole Attack (IBA)

The indirect black hole attack is used to lure traffic into the vicinity of a specified node in order to create a DOS attack and deplete the energy of that node. The attacker uses a powerful transmitter or directional antenna to tunnel RREP messages. An attacker puts the malicious node A near the destination node D. When a RREQ reaches destination D it sends a RREP packet towards the source node S. The malicious node A will then hear this RREP packet, and tunnels it directly to victim node V, which is near the source node. Due to tunneling, the RREP contains fewer hops. The victim node V then forwards the tunneled RREP towards the source node. The source node and all nearby nodes then mark victim node as their next hop towards destination. This creates a black hole, as the victim node V has an incomplete route towards destination and has to drop all packets that are sent to it by nearby nodes to forward to the destination node. When the legitimate RREP approaches the source node, it will be dropped by either the source node or by intermediate nodes as it contains a higher hop count to the destination [9].

2.5 Targeted Energy Depleting Wormhole Attack (TEDWA)

This variant of the wormhole attack is launched by using a single malicious node that has a powerful transmitter near the destination node. The purpose of this attack is to reduce the energy of a particular node in network. An attacker A does this by overhearing a RREP destined to a node S, and then tunnels this RREP to different parts of the network. In normal circumstances the RREP is only unicast to the source node through a single path. The attacker accomplishes fact that all nodes have a reverse route to source node, which has initiated route discovery. Due to tunneling of RREP to different parts of network, the source node receives multiple RREP packets from different nodes in network rather than a single RREP. In some cases if tunneled RREP reaches source node earlier than RREP through legitimate path then it can result in a DOS. This attack also affects those parts of the network where the attacker has tunneled the RREP, by creating multiple sinkholes.

3. RELATED WORK

(A) LEDS (Location-Aware End-to-end Data Security) seeks to provide end-to-end data security for event reports, as well as en-route bogus report filtering in WSNs [10]. In particular, it is designed to achieve the following goals:

i) **Provide end-to-end data confidentiality and authenticity:** both confidentiality and authenticity of event reports should be guaranteed as long as the sending nodes themselves are not compromised. Moreover, the impact of compromised nodes (if any) should be confined to their vicinity. The attacker cannot utilize the cryptographic materials obtained from compromised nodes to launch attacks at places other than the locations of the compromised nodes.

ii) **Achieve high-level of assurance on data availability:** 1) being resilient against report disruption attacks and selective forwarding attacks; 2) being able to early detect and drop bogus reports in an effective and deterministic manner.

(B) In [11] packet leashes are used to protect reactive routing protocols against wormhole attacks. A leash is defined as any information appended to a packet to restrict the maximum transmission distance of the packet. Two kinds of leashes have been proposed: geographical leashes and temporal leashes. In the geographical leash, the sender appends its location and the sending time to a packet. Based on this information, the receiving node computes an upper bound on the distance to the sender. This solution requires location information and coarse synchronization of all nodes in the network. In the temporal leash, the sender adds the sending time to the packet and the receiving node computes a traveling distance of that packet assuming propagation at the speed of light and using the difference between the sending time of packet and the receiving time of packet. This solution requires a fine grained synchronization among all nodes.

(C) Marti et al [12] introduced a monitoring mechanism known as watchdog to identify misbehaving nodes. In this approach, every sensor node has its own watchdog that monitors and records its one hop neighbors' behaviors. When a sender node S sends a packet to its neighbor node T, the watchdog in S verifies whether T forwards the packet toward the Base Station (BS) or not by using the sensor's overhearing ability within its transceiver range.

In this mechanism, S stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match. If yes, it means that the packet is forwarded by T and S will remove the packet from the buffer. If any packet stays in the buffer for a period longer than a per-determined time, the watchdog considers that T fails to forward the packet and will increase its failure score for T. If a neighbor's failure score exceeds a certain threshold number, it will be considered as a misbehaving node by S.

4. PROPOSED WORK

The wormhole attack is deployed using the routing protocol in network, thus detection of such attack in network is a complex task. Thus prevention scheme for improving security during path discovery is proposed based on contribution given in [13], where a different way to detect and prevent worm hole attack is provided by finding an alternative path.

According to [14] the basic idea of the technique is to discover alternative routes to a target node T that is one-hop neighbor's nodes that do not go through the wormhole. These alternative routes will be extensively dissimilar in length, means the length of the alternative path is greater than the paths that have wormhole attack, and otherwise the wormhole will not attract large amounts of traffic.

In order to provide an alternative and efficient approach than previous one, secure alternative path finding algorithm is given as

Assumption: an RTable = [p1, p2, p3… pm] which contains an entry of complete routing path p= {r1, r2, r3, …,rn}, similarly each route contains an sequence of next hop(as an aodv routing protocol contains).

Then

Input: RTable;

Output: alternate_path;

Initialization: hop1; hop2; count; //temporary variable

route; // an additional variable;

RTable = [p1, p2, p3…, pm]

pm=[r1,r2, r3,…,rn]

threshold;

process:

1. for(m=0;m<=1;m++)
2. {
3. route=RTable[m];
   a. for(n=0; n<=route.length(); n++)
   b. {
      i. P[n]=route;
      ii. if((rt->rt_hops != INFINITY2) && (rt ->rt_nexthop == id)// from reference [30]
      iii. {
         1. threshold= threshold+1;
      iv. }
      v. else
      vi. {
         1. threshold= threshold-1;
      vii. }
         1. if (counter=0)
         2. {
            a. hold1= threshold;
         3. }
         4. if(counter=1)
         5. {
            a. hold2= threshold;
            b. return;
         6. }
      viii. }
   b. }
4. }
5. if(hold1<hold2);
6. {
   c. //remove first route found in table thus we can write this as
   d. delete_entry[RTable[0]];
7. }

5. EXPERIMENTAL VIEW

In this study, we prepare a WSN where two nodes are communicating each other through a wireless channel. In this network, we deploy the wormhole attack and then prevent network from wormhole attack and compare the performance. To find and detection technique an important contribution is given in [15], where a different way to detect and prevent worm home attack is provided by using alternative path discovery.

According to [15] the basic idea of the technique is to discover alternative routes to a target node T that is one-hop neighbor's nodes that do not go through the wormhole. These alternative routes will be extensively dissimilar in length, means the length of the alternative path is greater than the path that have wormhole, and otherwise the wormhole will not attract large amounts of traffic.

Thus here we also provide an alternative and efficient approach than previous one, secure alternative path finding algorithm.

6. EXPERIMENTAL/NETWORK SETUP

6.1 Network Configuration

Parameters	**Value**
No. of nodes	25
Routing Protocol	AODV

Communication Scenario	CRB Traffic
MAC Layer	802.11
Channel	Wireless Channel
Simulation time	60 sec
Area	1000*1000

6.2 Simulation Scenario

In order to demonstrate the effect of wormhole attack in WSN two basic simulation scenarios are suggested to implement. Both of them are discussed as follows:

1. **Simulation of wormhole attack using AODV routing technique:** in this scenario the AODV routing is configured for communication and performance in terms of throughput is measured.
2. **Simulation of wormhole attack using enhanced routing protocol:** in this scenario AODV routing protocol is modified for implementing secure route discovery and performance is measured.

The figure 3 demonstrates simulation scenarios in both conditions, in this simulated network the wormhole link is simulated using red color nodes. In addition of that the green nodes are representing other routing nodes, for simulating effect of wormhole link a sender and receiver is implemented using the blue nodes.

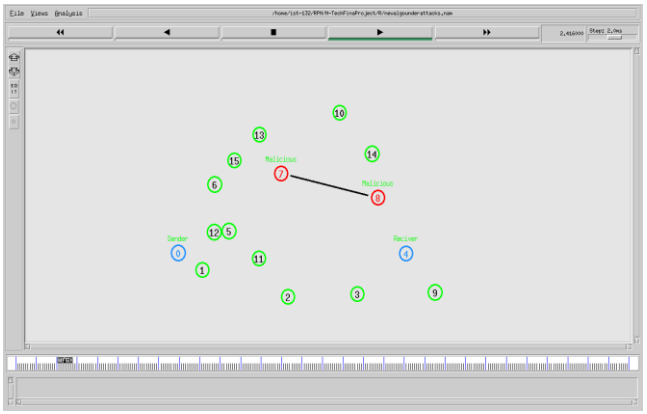

Fig. 3 Simulation Environment

7. RESULT ANALYSIS

This section provides the results of the developed secure routing protocol by performance and security analysis. Thus, according to the proposed simulation scenarios, two similar networks are configured with different routing techniques, first implemented with the traditional AODV protocol and second implemented with proposed routing protocol.

The wormhole link is deployed by modification of AODV routing protocol and performance in terms of throughput is measured. Throughput of the network is average rate of successfully delivered data over a communication channel. This data may be delivered over a logical or physical link, or pass through a certain node in network. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second. The estimated throughput for the given simulation scenario is given using figure 4.

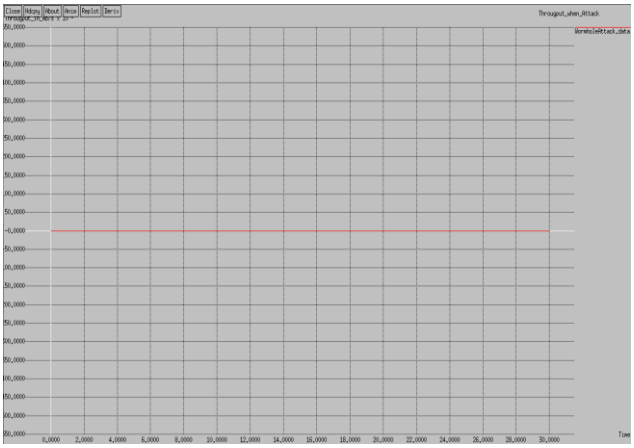

Fig. 4 Old AOVD under attack

In this diagram the performance of the routing protocol is constant and found that no bandwidth is consumed here. Thus, during wormhole attack attacker can affect the network performance. Thus no data is transmitted during attack deployment. On the other hand the performance of proposed routing protocol is given using figure 5, the obtained results shows that the throughput is varying with communication progress. Thus proposed routing protocol is able to prevent the effect of wormhole attack in network.

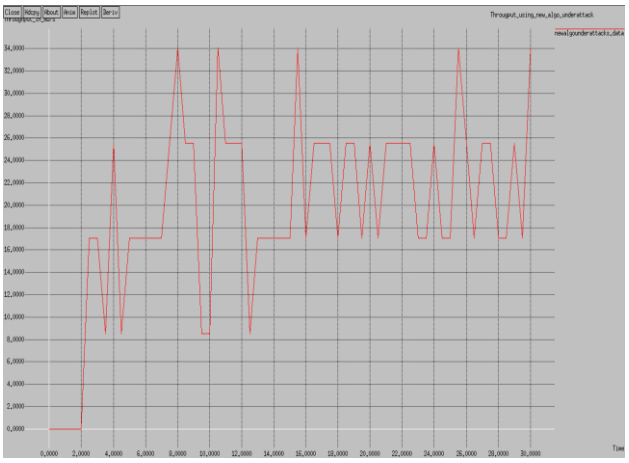

Fig. 5 Proposed Algorithm under attack

8. CONCLUSION AND FUTURE WORK

Due to mobility and their ad hoc configuration, wireless sensor network can be defined as wireless ad hoc network. Therefore, the network topology and the path discovery are dependent on their routing techniques. Thus performance and security is primary concern of the work. Thus first the investigation of routing protocols is performed. After observing different routing techniques that is concluded critical security issues are causes due to the poor routing strategy. Secondly different routing based attacks in WSN are investigated and finally a solution for wormhole attack is proposed.

Basically the wormhole link is promises to provide the shortest route in network. Thus most of the network traffic is attracted with this link, and the malicious node destroys all the communicated data in tunnel. Thus when a router discovers a path for communication a probability is made, the wormhole link is available in shortest path, thus an alternate path discovery methodology is implemented for the senders data packet transmission.

The implementation of proposed route discovery is given using NS2 network simulator. And performance of routing protocol is evaluated. The obtained results demonstrate the effectiveness of the preventive technique. Thus, the proposed routing technique is adoptable for secure route discovery process for preventing the wormhole attack in wireless sensor network.

8.1 Future work

The proposed method is a promising technique for secure path discovery during wormhole attack in wireless sensor networks. Thus that is extensible for preventing more attacks by including other contains in secure route discovery process. In order to improve more, the given technique can be implemented with threshold based concept for incorporating more than one attack prevention.

9. ACKNOWLEDGEMENT

With due respect we would like to inform, that the article which we had proposed is prepared for academic scenario, that is not feasible for industrial research purpose, the references which we had taken from listed here, one or not only references there are many other references which we had taken from real world and from daily life aspects. So it is vary through to remember all those references.

10. REFERENCES

[1] Rahul Patidar & Prof. Ritu Tandon, "A Survey of Wireless Sensor Network from Wormhole Security", National Conference on Advances in Computer Science & Technology, ACST-2014.

[2] John A. Stankovic, Wireless Sensor Networks, Department of Computer Science University of Virginia Charlottesville, Virginia 22904,June 19, 2006.

[3] Peng Ning and Kun Sun, Computer Science Department, North Carolina State University, A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols.

[4] L. Hu and D. Evans, Using Directional Antennas to Prevent Wormhole Attacks. In Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.

[5] Y. Hu, A. Perring, and D.B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In Proceedings of 22nd Annual Conference of the IEEE Computer and Communication Societies, Vol.3, April 2003. pp.1976-1986.

[6] A. Pirzada, and C. McDonald. Circumventing Sinkholes and Wormholes in Wireless Sensor Networks. International Work-shop on Wireless Ad Hoc networks, 2005(5):pp. 132-150.

[7] D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan, "A Recent Technique to Detect Sink Hole Attacks in WSN".

[8] Y. Hu, A. Perrig, D. Johnson, Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM 2003.

[9] Waqqas Sharif & Christopher Leckie, Department of Computer Science and Software Engineering The University of Melbourne Christopher Leckie, New Variants of Wormhole Attacks for Sensor Networks.

[10] Kui Ren, Wenjing Lou, Yanchao Zhang, LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks,

[11] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Attacks in Wireless Networks," In IEEE JSAC, Vol. 24, No. 2, Feb. 2006. pp. 370-380.

[12] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks," In Proc. Of International Conference on Mobile Computing and Networking (Mobicom), 2000, pp. 255-265.

[13] Devendra Singh Kushwaha, Ashish Khare, J. L .Rana, PhD, "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 62– No.7, January 2013.

[14] Anupama Sahu, Eduardo B. Fernandez, MihaelaCardei and Michael VanHilst, "A Pattern for a Sensor Node", Department of Computer and Electrical Engineering and Computer Science Florida Atlantic University, Boca Raton, FL 33431.

[15] Aashima Singla, Ratika Sachdeva, Review on Security Issues and Attacks in Wireless Sensor Networks, Volume3, Issue4, April-2013 ISSN: 2277.