IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

# A New Approach to Detect and Prevent Wormhole in Wireless Sensor Network Using AD-AODV

**N. Tamilarasi[1*], S.G. Santhi [2]**

[1]Dept. of Computer and Information Sciences, Annamalai University, Annamalainagar, India
[2]Dept. of Computer Science and Engineering, Annamalai University, Annamalainagar, India

*Corresponding Author: sjarasi08@gmail.com, Tel:9486638756*

**Available online at: www.ijcseonline.org**

Accepted: 26/Dec/2018, Published: 31/Dec/2018

***Abstract-***Now-a-days wireless networks are needed for mobile communication that makes wired communication impossible. The characteristics of WSN are small battery, restricted bandwidth and dynamic topology that expose Wireless Sensor Networks (WSN) to various kinds of attacks such as Black hole, Wormhole, Selective forwarding, Sink hole etc., . Therefore proper security measures will be taken while implementing WSN. Among all those attacks, wormhole attack is the most powerful attack in sensor networks. In this paper, a novelty routing protocol called attack detection ad hoc on demand distance vector (AD-AODV) is proposed to detect and prevent wormhole attack in wireless sensor network. This protocol needs no special hardware and software for the implementation. Moreover it is based on round trip time (RT), threshold round trip time (TRT) and the hop count for detecting the wormhole node. Network simulator2 (NS2) is used for implementing the proposed work.

***Keywords*** – Wireless sensor Network ,Round trip time, Threshold Round trip time, Hop count and AD-AODV

## I. INTRODUCTION

A wireless sensor network (WSN) is a scattered network and it consists of a large number of dispersed, independent, small, low powered devices called sensor nodes [1]. WSN logically enclose huge number of distinct, fixed devices that are networked for assembling, processing and also provide necessary data to the users and it has limited computing and processing ability. Sensor nodes have tiny micro controllers, which are used to send and receive the data all over the networks. Further, more the scalability of nodes in developed applications are extendable[2]. A group of sensor nodes gather the information from the ambience to achieve certain significant objectives. They communicate with one another in various configurations to reach the maximum performance. Sensor nodes communicate with one another using transceivers[3]. Hundreds or even thousands of sensor nodes are organized in WSN.

In recent years wireless sensor networks are used for many real time applications from house hold appliances to military applications, due to its technical progression in processor, efficient data transfer and minimum power consumption of embedded computing devices[4]. Sensor nodes aroused to examine ecological situations like temperature, pressure, moisture, noise, vibration, position etc[5].

In real time applications the nodes are performing various tasks like route discovery, smart sensing, information storage and processing, data gathering, finding destination, control and monitoring, location of nodes, organization and efficient routing between the sensor nodes and the base station[6].

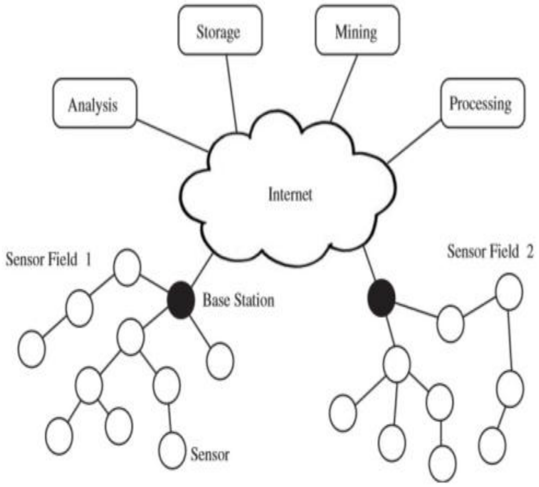


**Fig 1: Wireless sensor networks**

The major issues while implementing wireless network are mischievous aspects of sensor nodes .This happens due to variety of security attacks. In OSI reference model, among the seven layers network layer is responsible for routing attacks. Some of the probable network layer attacks are

Gray-Hole attack, Black Hole attack, Sybil attack, Sinkhole attack, and selective forwarding and wormhole attack. In this work an attempt is made for detection and avoidance of wormhole attack[7].

## II. WORMHOLE ATTACK

Wormhole attack is one of the most powerful attacks in the wireless sensor network. It creates confusion among routing mechanism which trusts on the understanding about distance between nodes. Moreover wormhole attack can easily be thrown by the invader without having sufficient knowledge of the wireless network or compromising any authentic nodes or cryptographic algorithms. The working principle of wormhole attack is to capture the data packet from one location to another location by creating a tunnel path between wormhole nodes[8]. It creates a routing faith between source and destination that only one or two hops were occurred during data transmission.

Wormhole attack has occurred in two modes (i) hidden mode and (ii) participation mode. In hidden mode, wormhole attack can be launched by packet encapsulation and packet relay methods. In participation mode, it can be thrown by high power transmission and out-of-band. Wormhole attack results in selective packet drop, routing disruption, information leakage and other more aggressive attacks. One of the best solutions to prevent and detect wormhole attack is transmission time based mechanism.

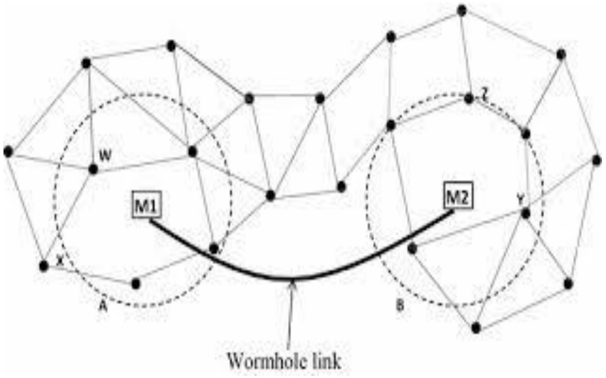


**Fig.2: Wormhole Attack**

In this paper the authors proposed a novelty protocol called attack detection ad hoc on demand distance vector (AD-AODV) routing protocol for detecting and preventing wormhole attack in wireless sensor networks.

In Fig 2, suppose the destination y notices that the packet from the source S is transferred through the node A and B under hidden wormhole attack, while it believes that the packet is delivered via node a, m1, m2 and B under exposed wormhole attack.

## III. REVIEW OF LITERATURE

A numerous work has been carried out by the researchers to overcome the network layer attacks.

Yith-Chun Hu et al[9]. proposed a novel, efficient protocol called TIK to implement temporal 'packet leashes' in order to detect and defend wormhole attack. TIK can avoid wormhole attacks by controlling the packets to travel within the radio range or any specified range.

Majid khabbazian et al[10]. introduces an on-demand distance vector routing protocol which is robust and secure to monitor the wormhole attack thrown in the hidden (or) participation mode. In order to remove the faulty links, the proposed protocol uses fault reports, digital signatures and destination acknowledge. This protocol also prevents multipath attack by introducing a sequence of hash numbers in its route discovery phase.

Rubinder singh et al[11]. presented a wormhole resistant hybrid technique (WRHT) which is used to identify the presence of wormhole attack. WRHT combines the concept of watch dog and Delphi and confirms that the wormhole is not found in the sensor network.

Yurong Xu et al[12]. describe a distributed algorithm for wormhole detection, based on the distortions created in the network. It also detects the abnormalities caused by wormholes using 'diameter' feature. The major advantage is that it provides the locations of wormholes

Gu-Hsin lai et al[13]. proposed routing protocol for low power and lossy networks (RPL) for wormhole detection in sensor networks. To measure the distance, the rank of a node defined RPL is adopted. If unreasonable rank values are identified, then the proposed method discovers malicious activity has occurred.

## IV. ROLE OFAODV PROTOCOL IN AD-AODV

In the proposed scheme, the authors suggest AODV routing protocol which establishes the route only on demand[14][15]. If a node wants to transfer the data to some destination in the network, first it detects the existence of route. If possible forward the packet towards the route otherwise it creates a route discovery process.

The basic message set of AODV consists of:

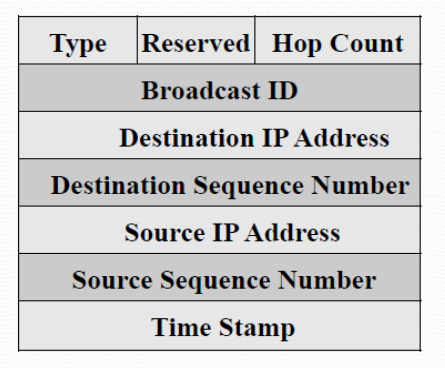
- RREQ – Route request
- RREP – Route reply
- RERR – Route error
- HELLO – For link status monitoring

*Route request*

The RREQ also includes the sequence number of the most recent destination node[16]. A legal destination route must contain a sequence number at least as large as that enclosed in the RREQ[17]. As a RREQ propagates at the entire network, intermediate nodes utilized to update their routing tables.

*Route reply*

When a destination is reached, it sends a route reply packet (RREP) to the source node, and all the intermediate nodes create its routing table towards forward path to the destination[18][19]. It consists of destination IP address of which the entry arrives.



| Type | Reserved | Hop Count |
|---|---|---|
| Broadcast ID | | |
| Destination IP Address | | |
| Destination Sequence Number | | |
| Source IP Address | | |
| Source Sequence Number | | |
| Time Stamp | | |

**Fig.3: AODV Packet Structure**

*Route error*

Accordingly, once the data packet reaches the destination, with the use of routing table entries, the data can be transferred[20]. On the other hand, the performance of recognized AODV has been inclined when a connection fails. In this manner the node detects the problem and sends a Route Error (RERR) message to the source node[21]. Later, the route discovery process will be restarted[22].

*Hello Messages*

A “Hello” message is send back to the source node, as a reply for the route request. This message is used for propagating connectivity information. An active node only can use “Hello” messages as part of it[23].

## V. WORKING MECHANISM OF AD-AODV

Attack Detection Ad hoc on Demand Distance Vector (AD-AODV) routing protocol is used to discover multiple paths between source and destination. Suppose a source wants to transmit a packet to some destination. The source has to check whether routing entries are available in the routing table or not. If it is present then use the path otherwise source node sends a Route Request Packet (RREQ) to all its neighbor nodes and it makes a note of sending time as T1. Once the neighbor receives the RREQ packet then it sends acknowledgement to the source via Route Reply packet (RREP). If more than one reply is received, then it is inferred that more than one route is available in the network to reach the destination and it is denoted as $T_{2\_1}$,$T_{2\_2,}$ $T_{2\_3}$……….. $T_{2\_k.}$ Next Round Trip Time is to be calculated by subtracting RREQ time from RREP time for each node in the path. The threshold round trip time can be calculated by taking the Round Trip Time of each route and divide it by their corresponding hop count. Then the average threshold round trip time is measured by adding the threshold round trip time of all the k paths and divide it by k. Check whether the threshold round trip time is less than the average threshold round trip time and the hop count for a particular $k^{th}$ path is equal to two then the $k^{th}$ is declared as wormhole attacked path. A dummy RREQ is send via $k^{th}$ path to destination and confirms that the node (M1) after immediate to source is wormhole and the node (M2) immediate before the destination is also a wormhole node. Discard the route by removing the entries M1 and M2 from the routing table and this message is to be broadcasted to all the nodes in the network as a routing alert.

## VI. PROPOSED ALGORITHM

```
1. For each route request packet transmitted by source node
      will be noted as time $T_1$
2. For every route reply acknowledged by the source node,
      will be noted as time $T_{2\_k}$.
3. Source node calculates the round trip time for all routes
      using a formula
      $RT_K = T_{2\_k} - T_1$
4. Calculate the threshold round trip time for all the k paths
      separately using the formula
            $TRT_k = \frac{RTK}{HCk}$
5. Then find the average threshold round trip time for all the
      k paths.
      $T_{avg\_k} = \frac{TRT1+TRT2+TRT3+ ……+TRTk}{k}$
   The above calculated $T_{avg\_k}$ is called threshold round trip
      time for the network.
6. If(($TRT_k<T_{avg\_k}$ )&&(hop count on route k== 2)) then
      {
   a. Route k is declared as wormhole attacked route.
   b. The source node identifies the first neighbour node M1
      as wormhole node.
   c. A dummy RREQ packet is sent by the source node
      through route k by M1.
   d. Destination node receives the dummy RREQ packet
      throughM2.
   e. Destination identifies its neighbour M2as wormhole
      node.
   f. The entries ofM1and M2are removed from the routing
      table and also advertised to further nodes in the
      network.
}
Else
{
         The path is declared as attacker free path.
}
```

**End If**

## VII. RESULTS AND DISCUSSIONS

The proposed AD-AODV is implemented in Network Simulator2 (NS2). About 500 sensor nodes are subject to attackers and the take results by varying the attackers as 10,20,30,40 and 50. The simulation is performed in the region 1000m x 1000m. Each sensor node has a Transmission range of 250m with Omni directional attenna, Two RayGround and the traffic source as Constant Bit Ratio(CBR). Sensor node transmit packets of size 1024 bytes with a rate of 80 kbps and the simulation takes 100 seconds for completion. Table 1 shows the simulation parameters.

**Table 1. Simulation Parameters**

| Parameter | Value |
|---|---|
| No. of Attack | 10, 20, 30, 40, 50 |
| Area Size | 1000m X 1000m |
| MAC TYPE | MAC / 802_11 |
| Propagation | TwoRayGround |
| Antenna | OmniAntenna |
| Interference range | 550 m |
| Transmission Range | 250m |
| Simulation Time | 100 sec |
| Traffic Source | CBR |
| Packet Size | 1024 bytes |
| Rate | 80 kbps |

Performance analysis of the proposed mechanism AD-AODV is calculated by varying the attackers size as 10,20,30,40 and 50. The performance metrics of the proposed approach AD-AODV and Existing AODV are discussed in the figures 4 – 8.The comparison of delay between the AD-AODV and the AODV is shown in figure 4. As the attacker increases in size,delay time of the sensor nodes also increases in the existing approach.But the proposed method decreases the delay to 45%. Next Packet Delivery Ratio is represented in the figure 5.By detecting the wormhole attack, one can avoid packet drop and increases the PDR .From the graph it is proved that AD-AODV approach is best than AODV.

Figure 6 shows the throughput of both existing and the proposed.From this we infer that attack free path increases the throughput.Figure 7 and 8 repersents the routing time and the network life time . If Routing time is minimum means , data is transmitted quickly then it saves the energy of the sensor node so the life time of the network will be increased.

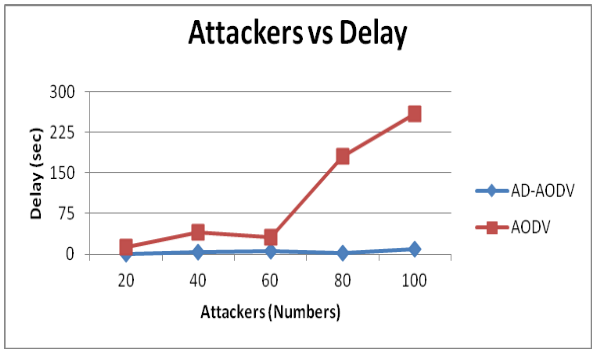


**Fig.4 Attackers vs Delay**

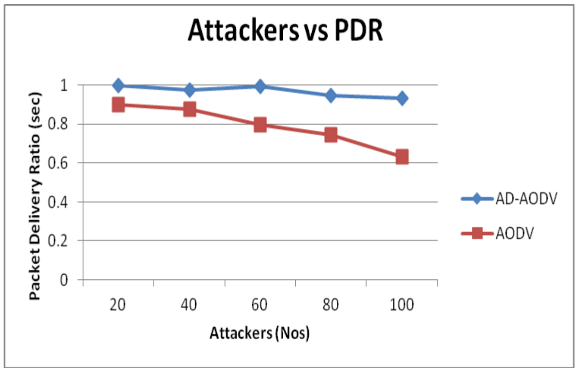


**Fig.5 Attackers vs Packet Delivery Ratio**

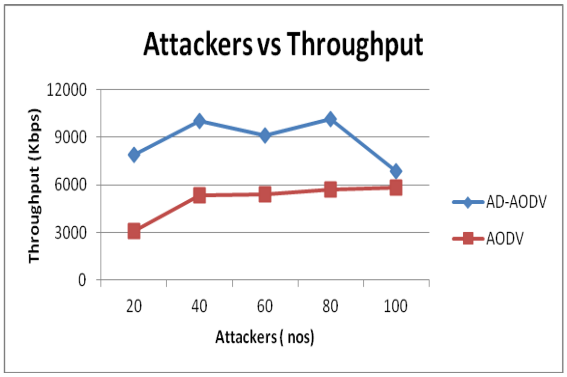


**Fig.6 Attackers vs Throughput**

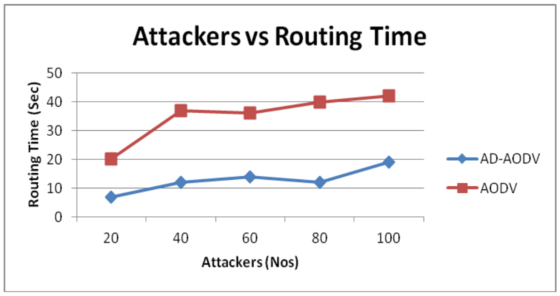


**Fig.7 Attackers vs Routing Time**

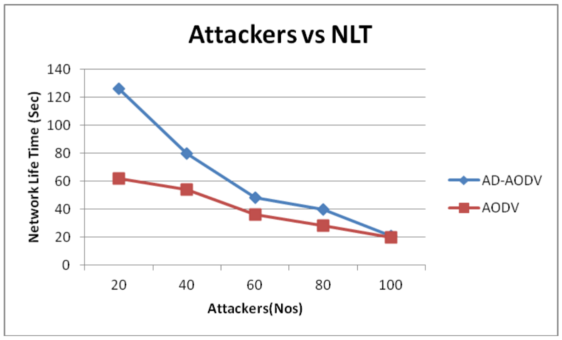


**Fig.8 Attackers vs Network Life Time**

## VIII. CONCLUSION

In this paper , it is proved that the proposed attack detection ad hoc on demand distance vector produces better results than existing protocol using Network Simulator 2 . The major advantage of AD-AODV is that no need of additional hardware and software is required while using this approach. Rather Round trip Time (RT) is calculated for every route. Then Threshold Round trip Time (TRT) is calculated from RT. Next finding average TRT using TRT , RT and Hop count . Comparing the K th route TRT with Average TRT and check whether Hop count is equal to 2, if it is true means then the route is identified as wormhole route otherwise it is declared as attacker free path. The simulation results confirms that the proposed AD-AODV shows better performance in various parameters like Throughput, Packet Delivery Ratio, Delay and Network Life Time than the existing AODV protocol.

## REFERENCES

[1] Zubair Ahmed Khan, M. Hasan Islam" Wormhole Attack: A new detection technique"978-1-4673-$^{4451}$- 7/12/$31.00 ©2012 IEEE.

[2] Perkins, C., Belding-Royer, E., & Das, S. (2002). "Adhoc on-demand distance vector (AODV) Routing",*IETF RFC 3561*, July 2002.

[3] Kanika Garg, RishiPal Singh, "Scheduling Algorithms in Mobile Ad Hoc Networks", July 2012

[4] R. Graaf, I. Hegazy, J. Horton, and R. Safavi-Naini. Distributed "Detection of wormhole attacks in wireless sensor networks," Springer book chapter Ad Hoc Networks, vol. 28, pp. 208í22, 2010. [34] A.Vani,

[5] D.Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), 2011, Vol. 3 No. 6, pp. 2377-2384, June 2011.

[6] H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

[7] S.Capkun, L. Buttyan, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," In Proc. of the first ACM workshop on Security of ad hoc and sensor networks, 2003.

[8] C. Nita-Rotaru, and H. Rubens, "An ondemand secure routing protocol resilient to byzantine failures," In ACM Workshop on Wireless Security (WiSe), 2002.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," In Proc. of INFOCOM, 2003.[9] Yith-Chun Hu" Wormhole attacks in wireless networks"IEEE Journal on Selected areas in Communication,IEEE Press Piscataway,NJ,USA ISSN:0733-8716 doi>10.1109/JSAC.2005.861394 Volume2,Issue 24,pages 370-380,

[10] Majid Khabbazian" Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure" V6T 1Z4

[11] Rupinder Singh, Jatinder Singh, and Ravinder Singh" WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks" Revised 23 October 2016; Accepted 2 November 2016

[12]Yurong Xu,Guanling Chen,James Ford,Fillia Makedon," Detecting Wormhole Attacks in Wireless Sensor Networks"Part of the IFIP International Federation for Information Processing book series (IFIPAICT, volume 253)

[13] Gu-Hsin" Detection of wormhole attacks on IPv6 mobility-based wireless sensor network", EURASIP Journal on Wireless Communications and Networking20162016:274 https://doi.org/10.1186/s13638-016-0776-0

[14] C. Nita-Rotaru, and H. Rubens, "An ondemand secure routing protocol resilient to byzantine failures," In ACM Workshop on Wireless Security (WiSe), 2002.

[15] B. Dahill, B. N. Levine, E. Royer, and C. Shields,, "A secure routing protocol for ad hoc networks," In Proc.of the 10th Conference on Network Protocols (ICNP), 2002.

[16] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," In Proc. of WCNC, 2005. [5] B. Awerbuch, D. Holmer.

[17] Haseed Zafar, David Harle, "QoS-aware Multipath Routing scheme for Mobile Ad Hoc Networks", April 2012.

[18] S. Capkun, L. Buttyan, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," In Proc. of the first ACM workshop on Security of ad hoc and sensor networks, 2003.

[19] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," ACM WiSe, 2002.

[20] W. Weichao, B. Bharat, Y. Lu, and X. Wu. "Defending against wormhole attacks in mobile ad-hoc networks," Wireless Communication and Mobile Computing, vol. 6, no. 4, pp 483í503, 2006.

[21] I. Khalil, S. Bagchi, and N.B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks," Elsevier Ad Hoc Networks, vol. 6, no. 3, pp. 344í62, 2008.

[22] R. Venkataraman, M. Pushpalatha, T.R. Rao, and R. Khemka. "A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad-hoc networks," International Journal of Recent Trends in Engineering, vol. 1, no. 2, May 2009.

[23] Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C.; , "DoS Attacks in Mobile Ad Hoc Networks: A Survey," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , vol., no., pp.535-541, 7-8 Jan. 2012.