Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 700 – 707

Procedia
Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol

Parmar Amish[a] ,V.B.Vaghela[b]

[a]*Student, Sankalchand Patel College of Engineering, Visnagar-384315, India*
[b]*Principal, Jashodaba Polytechnic Institute, Sidhpur-384151, India*

Abstract

Unique characteristics like limited bandwidth, limited battery power and dynamic topology makes Wireless sensor network (WSN) vulnerable to many kinds of attacks. Therefore interest in research of security in WSN has been increasing since last several years. 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. In this paper, 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. As compared to other solution shown in literature, proposed approach looks very promising. NS2 simulator is used to perform all simulation.

Keywords: WSN; Wormhole attack; RTT; AOMDV; malicious node.

1. Introduction

Sensor nodes are used to perform communication in wireless sensor network. Nodes in network here communicate directly with each other using wireless transceivers with no fixed infrastructure. Sensor nodes are deployed in large number to monitor the environment or system by measurement of physical parameters such as pressure, characteristic of object temperature and their relative humidity or motion. Each node of the sensor network consist of the three subsystems: the processing subsystem which performs local computations on the sensed data, the sensor subsystem which senses the environment and the communication subsystem which is responsible for message

* Corresponding author.
E-mail address: amish.heartly@gmail.com

doi:10.1016/j.procs.2016.03.092

interchange with neighbouring sensor nodes. Cost and size on sensor nodes result in corresponding constraints on resources such as memory, energy, computational speed and communications bandwidth. The application scenarios for WSNs are many including military surveillance, commercial, medical, manufacturing and home automation to name many but few [1]. Due to the broadcast nature of the transmission medium and fact that sensor nodes often operate in hostile environments WSNs are vulnerable to variety of security attacks.

According to the layers of the OSI model classification of security attacks in WSNs is done. The attacks which operate at the network layer are referred to as routing attacks.

There are many types of attacks possible in network layer like selective forwarding, spoofed or replayed routing information, Sybil attack, sinkhole attack, Hello flood attack and Wormhole attack.

Section II describes about wormhole attack in detail. Section III describes related work proposed by various authors. Section IV deliberates our proposed work for detection and prevention of wormhole attack. Section V we present our results. In section VI we conclude.

2. Wormhole Attack

This attack has one or more malicious node and a tunnel between them. The attacking nodes captures the packets from one location and transmits them to other distant located node which distributes them locally. The tunnel can be established in many ways e.g. in-band and out-of-band channel. 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 [2]. They can then launch a variety of attacks against the data traffic flow such as selective dropping, eavesdropping, replay attack, etc. Wormhole can be formed using, first, in-band channel packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in *Fig. 1*.

When malicious nodes form a wormhole they can disclose themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the latter is a hidden or close one.

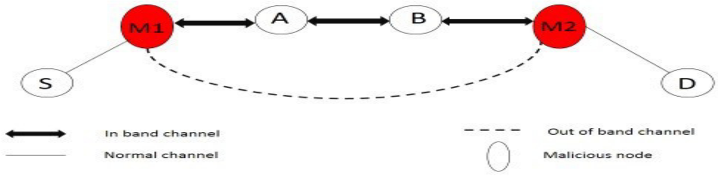


Fig 1 Wormhole Attack

In Fig 1, the destination D notice 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.

3. Related Work

In this section we discuss some of the prevailing solutions to the wormhole attacks in wireless ad hoc networks and mobile ad hoc networks. One of the solution is

S.Gupta et al [2] proposed a Wormhole Attack Detection Protocol using Hound packet called WHOP for detecting wormhole attacks without using monitoring system or any special hardware. A hound packet is used by source node after route discovery process to detect wormhole attacks which counts hop difference between the neighbours of the one hop away nodes in the route. The destination node detects the wormhole based on the hop after the process, difference between neighbours of nodes exceeds the acceptance level.

The technique called ‘packet leashes’ [3] prevents packets from traveling farther than radio transmission range. The wormhole attack can be detected by an unchangeable and independent physical metric, such as time delay or geographical location. It disables wormhole attack by restricting the maximum distance of transmission, using either local information or tight time synchronization. An upper bound on packets lifetime is ensured by the temporal leash. When a node sends a packet to the destination, the sending packet includes the time at which it send the packet and the receiving node compares this value to the time at which it received the packet. The recipient of the packet is within a certain distance from the sender is ensured by Geographical leash. The sending node location and its sending time is included in the sending packet. When they reach the receiving node computes the upper bound on the distance between the sender and its own. The drawback of temporal leashes is that they need highly synchronized clocks and of geographical leash is that, each node must know its own location and all nodes must have loosely synchronized clocks.

Chiu et al. [4] introduce a delay analysis approach called DELPHI. It applies a multi-path approach and records the delay and hope counts in transmitting RREQ and RREP through the paths. It calculates mean delay per hop of every possible route. The sender computes mean delay per hop of each route after collecting all response. In path with the wormhole attacks, the delay would be obviously longer than the normal path with the same hop count. Hence, wormhole nodes could be avoided if the path with longer delays would not be selected to transmit the data packet.

Khalil et al. [5] introduces LITEWORP in which they used notion of guard node. If one of the neighbour of guard node behaves maliciously it can detect the wormhole. The guard node is a common neighbour of two nodes to detect a legitimate link between them. However it is not always possible to find a guard node for a particular link in a sparse network.

Varsha et al. [6] presented efficient method to detect a wormhole attack called modified wormhole detection AODV protocol (MAODV). Based on number of hops and delay of each node in different paths from source to destination wormhole attack is detected. It compares the delay per hop of every node in the normal path and a path that is under wormhole attack, finds that delay per hop of a path that is wormhole attack is larger in comparison of normal path. Advantages of this method are that it requires no special hardware and it do not require positioning system and clock synchronization. Shortcoming is that when all the paths are wormhole affected this method does not work well.

4. Proposed mechanism to detect and prevent wormhole attack

To discover multiple paths between the source and the destination in every route discovery Ad-hoc on-demand Multipath Distance Vector routing protocol (AOMDV) is used which is an extension of the AODV protocol. In AOMDV routing protocol the sender node checks in the route table whether a route is present or not for communication of any two nodes, if present it gives the routing information else it broadcasts the packet, if the route is not present then it broadcasts the RREQ packet to its neighbours which in turn checks whether a route is present to the required destination or not. Whenever the destination receives the RREQ packet it sends RREP packet to the source along the same path through which the RREQ packet has arrived. For all RREQ packets arrived through other routes the RREP packets are sent along the same path. All the paths are stored in the routing table at source node. In this way the routes are established [7]. The main idea in AOMDV is during route discovery procedure to compute multiple paths for contending link failure. When AOMDV builds multiple paths, it will select the main path for data transmission which is based on the time of routing establishment. Only when the main path is down other paths can be effective and the earliest one will be regarded the best one.

Using AOMDV protocol in this paper a technique is proposed to detect and prevent the wormhole attack in the network efficiently. Details of the proposed algorithm is as follows. When the source node broadcasts a RREQ packet note time t_1 and when the corresponding RREP packet is received by the source, again note the received time of the packet. If multiple RREP packets received, that means there is more than one route available to the destination node then note the corresponding times t_{2_i} of each RREP packet. By using the above two values one can calculate the round trip time t_{3_i} of the established route or routes [8].

Take Round Trip Time of each route t_{3_i} and divide it by respective hop count. Calculate the average round trip time of all the routes with the help of this value say t_{s_i}. The value obtained is threshold Round Trip Time t_{th}. After comparing the threshold value with each Round Trip Time t_{s_i} ,if the total Round Trip Time t_{s_i} is fewer than threshold Round Trip Time t_{th} and hop count of that particular i^{th} route is equal to two than wormhole link is existing in that route else no wormhole link present in that route. Since wormhole link spotted in that route, sender detects first neighbour node m_1 as wormhole node and sends dummy RREQ packet through that route i and neighbour m_1. At the destination end receiver receives dummy RREQ packet from its neighbour m_2 and detects neighbour m_2 as wormhole node. Routing entries for m_1 and m_2 are removed from the source node and broadcast to other nodes. Thus wormhole affected link is jammed and is no more used. So, that from the next time onwards whenever a source node needs a route to that destination, first it checks in the routing table in the route established phase for a route and it will come to know that, the route is having wormhole link and it will not take that route instead it will take another route from the routing list of the source node which is free from wormhole link if available. Benefit of using AOMDV protocol in our proposed mechanism is that, it has less overhead and end to end delay. Fig. 2 shows the flow chart of proposed algorithm.

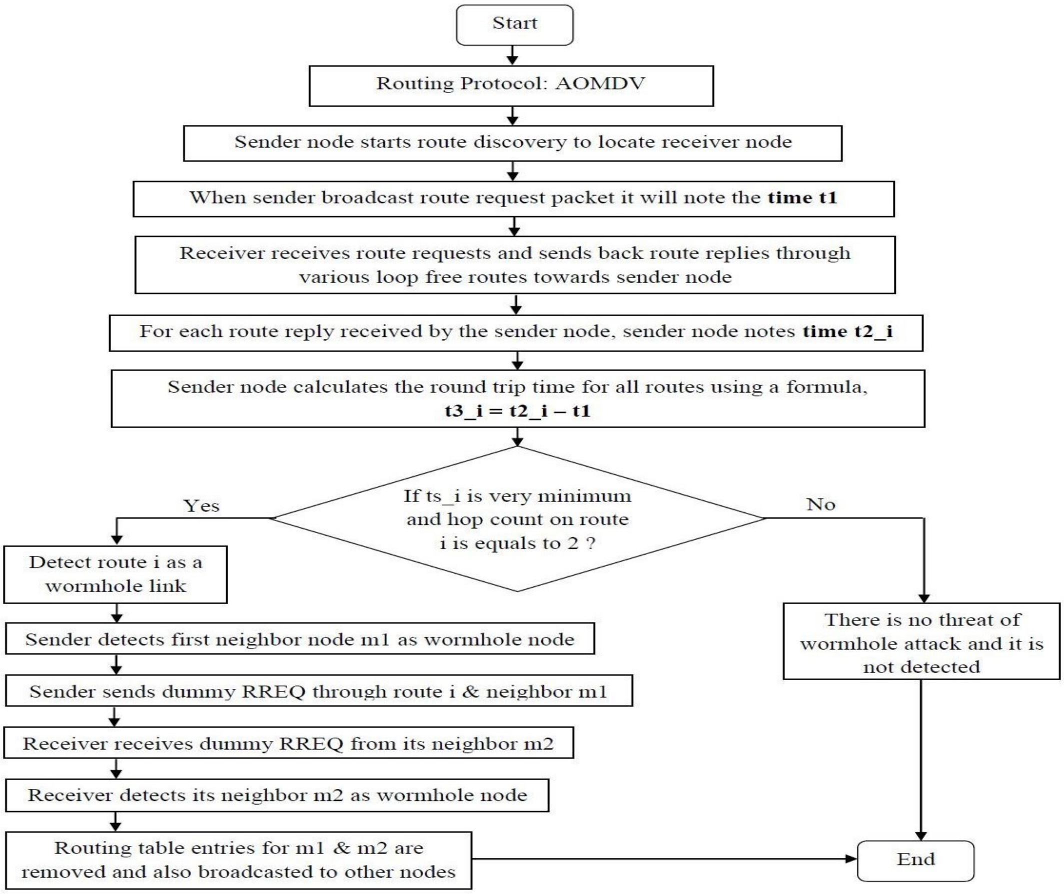

Start
Routing Protocol: AOMDV
Sender node starts route discovery to locate receiver node
When sender broadcast route request packet it will note the **time t1**
Receiver receives route requests and sends back route replies through various loop free routes towards sender node
For each route reply received by the sender node, sender node notes **time t2_i**
Sender node calculates the round trip time for all routes using a formula, **t3_i = t2_i – t1**
If ts_i is very minimum and hop count on route i is equals to 2 ?
Yes
No
Detect route i as a wormhole link
Sender detects first neighbor node m1 as wormhole node
Sender sends dummy RREQ through route i & neighbor m1
Receiver receives dummy RREQ from its neighbor m2
Receiver detects its neighbor m2 as wormhole node
Routing table entries for m1 & m2 are removed and also broadcasted to other nodes
There is no threat of wormhole attack and it is not detected
End

Fig 2 Flow chart of proposed algorithm

Algorithm:

```
1. When sender broadcast route request packet it will note the time $t_1$.
2. For each route reply received by the sender node, sender node notes time $t_{2\_i}$.
3. Sender node calculates the round trip time for all routes using a formula
   $t_{3\_i}$ = $t_{2\_i}$-$t_1$.
4. Calculate the threshold round trip time by using this formula
   $\frac{t_{3\_i}}{hop\ count_i} = t_{s\_i}$
5. Take average of $t_{s\_i}$ for i number of paths from step 4.
6. Note this time as threshold round trip time $t_{th}$ for each route.
   [Just to understand assume i=3 i.e. total three paths to the destination. Then according to step 4
   $\frac{t_{3\_1}}{hop\ count_1} = t_{s\_1}$, $\frac{t_{3\_2}}{hop\ count_2} = t_{s\_2}$, $\frac{t_{3\_3}}{hop\ count_3} = t_{s\_3}$

   Step 5 will give the average of above values
   $\frac{t_{s\_1}+t_{s\_2}+t_{s\_3}}{3}$ = $t_{th}$ which is threshold round trip time ]
7. If ($t_{s\_i}$ is less than $t_{th}$ and hop count on route i is equals to 2 == true) then{
      a. Detect route i as a wormhole link
      b. Sender detects first neighbour node $m_1$ as wormhole node
      c. Sender sends dummy RREQ through route i and neighbour $m_1$
      d. Receiver receives dummy RREQ from its neighbour $m_2$
      e. Receiver detects its neighbour $m_2$ as wormhole node
      f. Routing table entries for $m_1$ and $m_2$ are removed and also broadcasted to other nodes
}
Else {
   There is no threat of wormhole attack and it is not detected
   }
End If
```

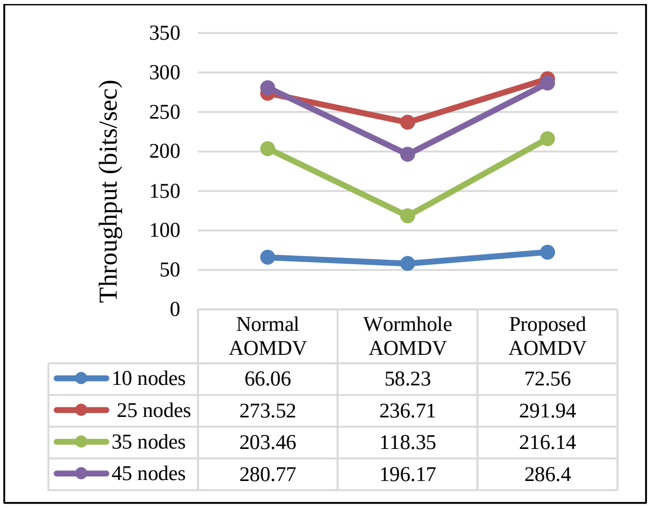
5. SIMULATION ENVIRONMENT AND RESULTS

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 by comparing normal AOMDV, wormhole affected AOMDV and proposed AOMDV protocols in a network. Initially the readings of normal AOMDV are noted based on above described parameters for 10, 25, 35 and 45 nodes respectively. Then the wormhole nodes are added in Normal conditions and results are noted again. Lastly, proposed method is applied in the infectious network and results are compared for all the three scenarios. The wireless sensor network environment is formed using network simulator-2.34. The following table indicates the simulation parameters.

Table 1 Simulation Parameters

Simulation area	500m x 500m
Routing protocol	AOMDV
Packet size	512 bytes
Traffic Rate	CBR
Number of nodes	10, 25, 35, 45
Range of transmission	230m
Simulation time	200s
Mobility model	Fixed

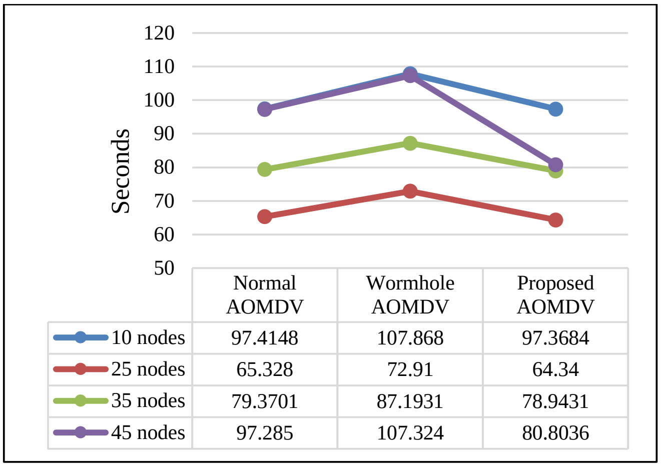
In all figures below on x-axis are the parameters and on y-axis are the routing protocols. Fig. 3. shows that the values of average throughput are plotted against three routing protocols for network density (nodes). The difference in the value of throughput of protocol proposed AOMDV and wormhole AOMDV increases as the network density rises. Thus in terms of throughput as a parameter the performance of network by given proposed algorithm increases for dense network.



	Normal AOMDV	Wormhole AOMDV	Proposed AOMDV
10 nodes	66.06	58.23	72.56
25 nodes	273.52	236.71	291.94
35 nodes	203.46	118.35	216.14
45 nodes	280.77	196.17	286.4

Fig 3 Average throughput for 10, 25, 35 and 45 nodes

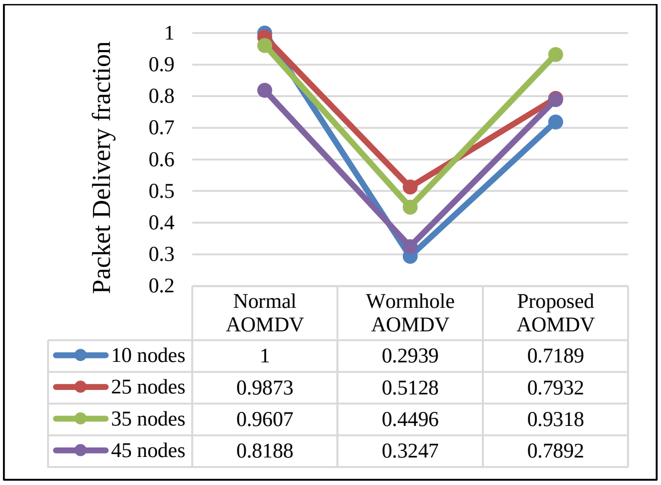
In fig. 4. note that when wormhole nodes are kept in normal AOMDV it increases the average end to end delay of the network. After applying proposed algorithm in this environment the average end to end delay value decreases. The values of delay obtained in proposed AOMDV are even less than normal AOMDV. The above values in the fig. 4. depicts that the average end to end parameter is improved for large density network.



	Normal AOMDV	Wormhole AOMDV	Proposed AOMDV
10 nodes	97.4148	107.868	97.3684
25 nodes	65.328	72.91	64.34
35 nodes	79.3701	87.1931	78.9431
45 nodes	97.285	107.324	80.8036

Fig 4 Average end to end delay for 10, 25, 35 and 45 nodes

The results for packet delivery fraction in fig. 5. shows that in spite of variations the packet delivery fraction for the different network densities improves. Here it can be seen easily by taking difference of wormhole AOMDV and proposed AOMDV.



	Normal AOMDV	Wormhole AOMDV	Proposed AOMDV
10 nodes	1	0.2939	0.7189
25 nodes	0.9873	0.5128	0.7932
35 nodes	0.9607	0.4496	0.9318
45 nodes	0.8188	0.3247	0.7892

Fig 5 Packet delivery fraction for 10, 25, 35 and 45 nodes

6. Conclusion

In this work, we have proposed and implemented a wormhole detection and prevention mechanism to detect and prevent the wormhole attacks. In our technique, no special hardware is required. All we have done is calculated the 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. In future this proposed method can be implemented in mobile ad hoc network also.

References

1. C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks-Architecture and Protocols," Prentice Hall PTR, Theodore S. Rappaport, Series editor.
2. S. Gupta, S. Kar and S. Dharmaraja, "WHOP: wormhole Attack Detection protocol using hound packet". In the international conference on innovations Technology, IEEE, pp. 226-231, April 2011.
3. Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE journal on selected areas in communications, Vol.24, No.2, pp. 370-380,February 2006.
4. H.S. Chiu and K.S. Lui. DELPHI, "Wormhole detection mechanism for ad hoc wireless networks", 1st International Symposium on Wireless Pervasive Computing, pp. 6–11, January 2006.
5. Umesh kumar chaurasia and Mrs. Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol", IEEE, pp. 239-243, 2013.
6. Khalil S. Bagchi and N.B. Shroff. LITEWORP, "A lightweight countermeasure for the wormhole attack in multihop wireless networks", International Conference on Dependable Systems and Networks (ICDSN), pp. 612-621, 2005.
7. S. R. Biradar, Koushik Majumder, Subir Kumar Sarkar, Puttamadappa S.R.Biradar, "Performance Evaluation and Comparison of AODV and AOMDV", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 02, pp. 373-377, 2010.
8. V.karthik raju and K. vinay kumar. "A simple and efficient mechanism to detect and avoid wormhole attacke in mobile ad hoc networks", International conference on computing sciences, pp. 271-275, IEEE 2012.