IJITKM Volume 7 • Number 1 • December 2013 pp. 81-86 (ISSN 0973-4414)

Analysis and Implementation of Proposed Hybrid H-AODV Routing Protocol of MANETs using Detection of Malicious Nodes in the Network

Harsha Tamboli,Dr. Deepak Dembla
Researvh Scholar, Deptt. of CSE, Arya Institute of Engg. & Technology, Jaipur
Prof. & HOD, Deptt. Of CSE, Arya Institute of Engg. & Technology, Jaipur
tharsha19@gmail.com, deepak_dembla@yahoo.com

Abstract- A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes which can freely and dynamically self-organize and co-operative in to arbitrary and temporary network topologies. Security of AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. If there are multiple malicious nodes in a network and are co-operating with each other then it is known as "co-operative black hole attack". In this work a hybrid approach is proposed for implementing H-AODV, by preventing malicious nodes from network and improving efficiency. The proposed H-AODV protocol is simulated on ns-3 simulator and results are compared and analysed with base AODV protocol, based on important performance metrics like packet delivery fraction, end-to-end delay and throughput. It is concluded from the result that H-AODV with proposed enhancement is comparably better than AODV (under attack) for performance measures like packet delivery fraction, packet drop ratio, end to end delay and throughput. The performance of the detection is significantly improved and delay in detection and prevention is also reduced.

I. INTRODUCTION

A MANET is referred as an infrastructure less network because the mobile nodes in the network dynamically locate paths among themselves to transfer packets provisionally [2] or a collection of wireless nodes communicating in a confined wireless environment in the absence of any centralized organization and any fixed infrastructure, is known as a mobile ad hoc network (MANET) [3].There are various routing protocol available for this changing topology network. As routers are free to move and allowed to join a network range anytime, so MANET networks are more vulnerable to attacks. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc On Demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1].

1.1 AODV (Ad hoc On demand Distance Vector)

AODV is a state-of-the-art routing protocol that adopts a purely reactive strategy [4] and is similar to DSR protocol in which routes are determined only when needed. But in AODV hello messages are used to detect and monitor links to neighbours. Hello messages are way of acknowledging that the neighbouring node is active. When a source has data to transmit to an unknown destination, or the destination whose route from source is not known, it conducts a route discovery procedure. In route discovery procedure it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP).

1.2 BLACK HOLE ATTACK

In this type of attack, malicious node claims having an optimum route to the node whose packets it wants to intercept [5], but in real they do not have that route to forward packet to destination. Malicious nodes degrade the performance of network eventually by participating in the network actively. If there are multiple malicious nodes in the network, and are cooperating with each other for performing the attack than such attack is called Cooperative Black Hole attack These nodes falsely replies for route requests without having an active route to the destination and exploits the protocol to advertise itself as having a good and valid path to a destination node, as a result all the data packets are consumed by it or lost.

II. BACKGROUND AND RELATED WORK

In some hostile and suspicious settings, node identities must not be exposed and node movements should be untraceable. This paper is given by ***[Karim 2011]***, [6], and address a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link state based routing protocol (ALARM).A similar domain study is conducted by ***[Ziming 2012]*** [7] according to author existing solutions typically attempt to isolate malicious nodes based on binary or native fuzzy response decisions. ***[Nital 2010]***[4] AODV is a state-of-the-art routing protocol that adopts a purely reactive strategy: it

sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route DiHovery phase and Route Error (RER) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in[8]. Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated afresh, too. The fallout is that there is a high probability of a malicious node attempting to orchestrate the Black hole attacks in AODV.

III. PROBLEM STATEMENT

MANET characteristic acquire many security challenges. There are certain attack from literature and found that malicious nodes have harmful effect on network, as they consume data packets by claiming through a RREP route reply message message that the malicious node is having a route between source and destination. The presence of attack and congestion degrades the performance in terms of security and efficiency. There are various solution previously proposed and implemented for preventing co-operative black hole attack. But most of them are not much effective due to their performance or accuracy.

IV. IMPLEMENTATION METHODOLOGY

In this work a hybrid approach is proposed for implementing H-AODV, by preventing malicious nodes from network and improving efficiency. And this hybrid approach is a combination of the concept of fidelity level, for finding malicious node, and ECARP technique for efficiency consideration. The value of fidelity level can be computed as:

$$\text{FIDELITY} = \frac{number\ of\ forward\ packets}{number\ of\ received\ packets}$$

This level contains a Boolean value like 0 or 1. If fidelity field in routing table of H-AODV contains 0, it indicates that H-AODV found a malicious entry in network, which may be harmful for network, H-AODV delete this entry, otherwise considered as safe route. But using only fidelity level concept introduces some end-to-end delay for data delivery. There is one more fact for packet drop and delay, that is congestion, [9]. Congestion means where the number of packets in the queue is more than buffer length of the device. If the length is more than fixed size, than all the packets dropped and introduce delay. Here the solution is to divert traffic to other route if possible. For this a variable is introduced called congestion level Cs. Can be calculated as:

$$Cs = \frac{Number\ of\ buffered\ packets\ in\ buffer}{max\ buffer\ size}$$

If the value of congestion level is greater than a particular threshold value, than another different route is selected.

4.1 Implementation

For the prevention of malicious activity in network, a hybrid scheme is used for implementing H-AODV routing protocol and is simulated using NS3 network simulator. For this study the algorithm is simulated in NS3 simulator. NS-3 is a discrete-event network simulator, targeted primarily for research and educational use. NS-3 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use.

4.2 Proposed Algorithm

Step-1 Finding path from source to destination.
Step-2 Calculate Fidelity level value and congestion level value.
Step-3 Compare the average of fidelity level of requested node and next hop with threshold value.
Step-4 If average is greater than threshold value send data packet.
Step-5 Compare congestion value with a particular threshold value.
Step-6 If congestion is less than a particular threshold value than choose another path.
Step-7 If acknowledgement of data packets is not received within a particular time then decrement fidelity level.
Step-8 If fidelity level value is zero then node claiming route is considered as malicious and the node is deleted.

4.3 Snippet of Modified Code for Proposed H-AODV Protocol

Small code snippet is shown below:

```
RoutingProtocol::SendHello() {
   NS_LOG_FUNCTION(this);
  int bufp =  m_queue.GetSize();
  int bufs =  m_queue.GetMaxQueueLen();
  int cs =  bufp/bufs;
  if(cs<=1/2){
     return 1; }
   else
     if((cs>=1/2) ||(cs<=3/4)){
  }
     else  if((cs>=3/4) ||(cs<=1)){
      m_routingTable.Purge();
  }
   for (std::map<Ptr<Socket>, Ipv4InterfaceAddress>::const_iterator j = m_socketAddresses.begin(); j !=
m_socketAddresses.end(); ++j) {
      Ptr<Socket> socket = j->first;
      Ipv4InterfaceAddress iface = j->second;
      RrepHeader helloHeader( 0,  0,  iface.GetLocal(),  m_seqNo,
      packet->AddHeader(tHeader);
      Ipv4Address destination;
      if (iface.GetMask() == Ipv4Mask::GetOnes()) {
         destination = Ipv4Address("255.255.255.255");
      } else {
         destination = iface.GetBroadcast();
      }
      socket->SendTo(packet, 0, InetSocketAddress(destination, AODV_PORT));
   } }
```

V. SIMULATION SETUP

The performance is analyzed for the parameters like packet delivery fraction, packet drop ratio, end to end delay and throughput. Both the AODV (under attack) and H-AODV are simulated in ns-3 simulator in same settings of parameters and scenarios. To prepare simulation for desired network utility we provide the following given simulation setup.

Table 5.1 Simulation setup

Simulator	NS3
Simulation time	500ms
Loss Model	Range Propagation model
Routing protocol	AODV
Simulation size	1000*1000
Number of node	10
Channel	WiFi
Traffic	UDP

VI. RESULT AND ANALYSIS

In this topic the results are shown for the comparison of AODV with H-AODV for few performance parameters.

6.1Packet Drop Ratio Analysis

Provides the number of packets drop during communication sessions [10].

Fig 6.1shows the analysis of packet delivery ratio for AODV (under attack) and H-AODV, it is found that H-AODV outperforms AODV (under attack). The main reason for packet drop is availability of malicious node in the network and congestion, under attack condition the malicious nodes are available hence they consume the data packets routed toward destination, so number of packet drop increases in each session of communication.

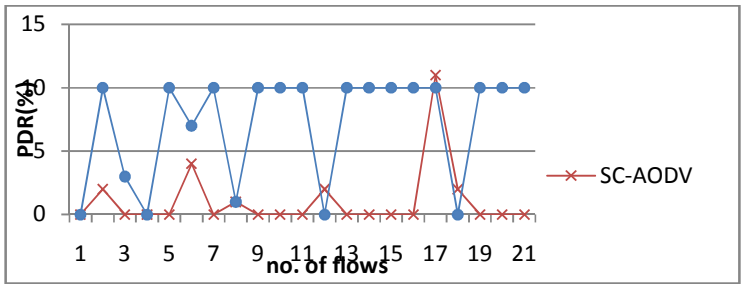

Fig. 6.1 AODV (under attack condition) VS. H-AODV for PDR

After implementation of the proposed method in AODV protocol it is found that packet drop ratio decreases as the malicious node are detected and removed, and the dropping of packet due to congestion is also removed and it is found that the PDR is effectively improved using the proposed technique of detection and prevention of attack.

4.2 Packet Delivery Fraction Analysis

The ratio of the data packets delivered to the Destinations to those generated by the constant bit rate sources is packet delivery fraction. Packets delivered and packets missing are taking in to reflection [11].

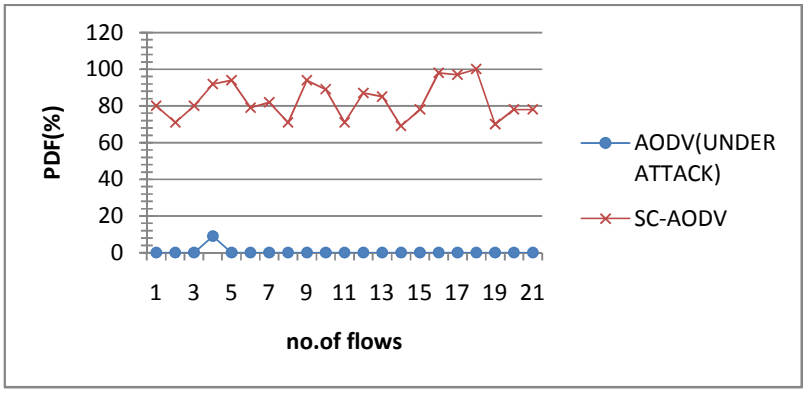

Fig. 6.2 AODV (under attack condition) VS. H-AODV for PDF

After implementing the proposed technique the malicious nodes are removed and congestion level is checked; which in turn results in more packets reaches towards the destination end as packets are not dropped and even not consumed, hence packet delivery fraction increases. It also implies that packet drop ratio is inversely proportional to packet delivery fraction. This is concluded from figure 6.2 for packet delivery fraction that H-AODV outperforms AODV (under attack) by using this method.

6.3 End To End Delay Analysis

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. It is observed from figure that 6.3, for H-AODV the average end to end delay decreases as compared to AODV (under attack).

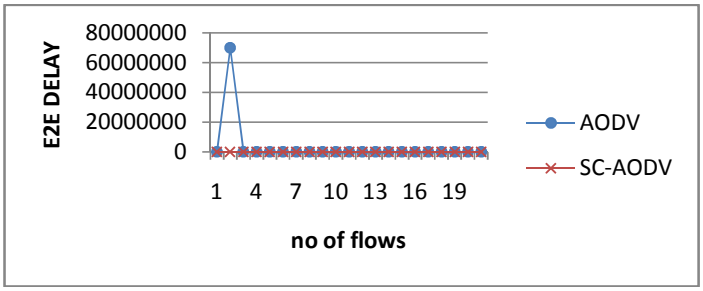

Fig. 6.3 AODV (under attack) VS. H-AODV (with proposed algorithm) for End to End Delay

In the case of AODV (under attack) the nodes have to wait for additional time before sending the reply while in H-AODV the waiting time is removed and S-AODV also chooses another route in the presence of congestion.

6.4. Throughput Analysis

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

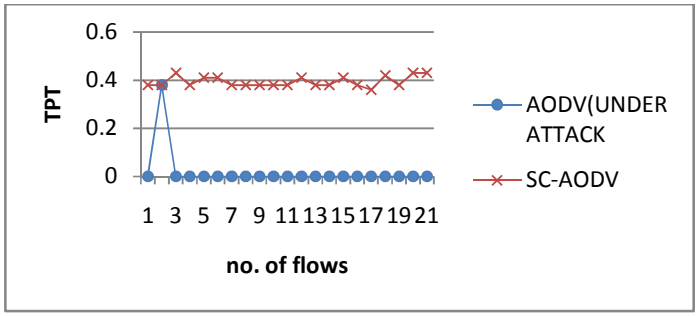

Fig. 6.4 AODV (under attack) VS. H-AODV (with proposed algorithm) for Throughput

After implementing the proposed technique the conclusion is that throughput is improved adoptively and provides the efficient results. The overall comparison is shown in fig 6.4. When attack is formed the network throughput becomes zero on increasing number of flows. As concluded H-AODV is better than AODV in terms of throughput.

VII. CONCLUSION AND FUTURE WORK

It is found in this research work that the hybrid H-AODV protocol performs better than traditional AODV routing protocol of MANET, which is not very much secured and is threat prone. The main conclusion of the above research work is packet drop ratio, packet delivery fraction, and end to end delay and throughput parameters. If we remove the malicious nodes and include the concept of the congestion level the packet drop ratio decreases as consumption of packet by malicious node is removed; hence packet delivery fraction increases as more nodes reaches destination. And it is concluded that performance of throughput has been improved and hence it gives high performance. On analysis E2E delay it is found that is reduced which increases the performance. Finally it has been concluded that the performance of the detection is improved approximately 5-10% and delay in detection and prevention is reduced. This concept is able to detect only one attack and able to detect and prevent the black hole and in some cases of DOS attacks. In future a normalized framework for security can be created for more than one attack and routing protocol.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "*Routing Security in Wireless Ad Hoc Networks*", University ofCincinnati, IEEE Communications magazine,Vol.40, no.10, October 2002.

[2] Jim Dowling, Eoin Curran, Raymond Cunningham, and Vinny Cahill ,"Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing" , *IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans*, VOL. 35, NO. 3, MAY 2005

[3] Rooshabh Kothari and Deepak Dembla," Performance Analysis & Implementation of Enhanced DSR Routing Protocol of MANET using Selfish behaviour", *International Journal of Advanced Research in Computer Hience and Software Engineering* , Volume 3, Issue 7, July 2013,pp 896-901, ISSN: 2277 128X

[4] Nital mistry et. al, Improving AODV Protocol against Blackhole Attacks", Proceedings of the international Multiconferece of Engineers and computer Hientists",vol-II 2010, IMECS 2010,march 17-19.

[5] Gagandeep, Aashima, PawanKumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[6] Karim El Defrawy, Member, Gene Tsudik,"ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE *journal on selected areas in communications*, VOL. 29, NO. 10, DECEMBER 2011

[7] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu, " Risk-Aware Mitigation for MANET Routing Attacks", *IEEE transactions on dependable and secure computing*, VOL. 9, NO. 2, MARCH/APRIL 2012

[8] C. Perkins. "(RFC) request for Comments-3561", Category:Experimental, Network, Working Group, July 2003.

[9] Subir Kumar Sarkar,et. Al., "ECARP: An Efficient Congestion Adaptive Routing Protocol for Mobile Ad hoc Networks",*6th International Conference on ITS Telecommunications Proceedings, 2006*

[10] Nilesh P. Bobade1, Nitiket N. Mhala2 "Performance Evaluation Of Aodv and DSR On-Demand Routing Protocols With Varying Manet Size", *International Journal of Wireless & Mobile Networks (IJWMN),* Vol. 4, No. 1, February 2012.

[11] G.L.Saini,Dr. Deepak Dembla, " Modeling, Implementation and Performance Evaluation of E-AODV Routing Protocol in MANETs", *International Journal of Advanced Research in Computer Hience and Software Engineering,* Volume 3, Issue 7, July 2013, pp1221-1227 ,ISSN: 2277 128X, 2013.