International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 31, Issue 01) and (Publishing Month: June 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN: 2319-6564
www.ijesonline.com

CBRM-AODV: A Countermeasure Technique to Handle Collaborative and Cooperative Attacks on Network Layer

Ishita Sharma[1] and Taruna Sikka[2]

[1]M.Tech. Scholar, ECE Department, SPGOI, Rohtak, Haryana (India)
sharmaishita1992@gmail.com
[2]Assistant Professor, ECE Department, SPGOI, Rohtak, Haryana (India)

Publishing Date: June 29, 2016

Abstract

Ad hoc networks gain popularity due to their vast application in different areas. The popularity gain also increases security risk. Various layer-wise attacks exist to degrade the performance of routing protocols in the ad hoc network. This paper handles the network layer attack particularly blackhole, wormhole and grayhole attack in the AODV routing protocol. This paper designs a technique to handle the collaborative and cooperative network layer attacks. The result analysis on different network shows the significance of the technique as improved PDR, throughput achieved even in the presence of attacks.

Keywords: *Blackhole, Wormhole, Grayhole, AODV, Security.*

1. Introduction

Ad Hoc Networks are the autonomous networks that use wireless communication technology in multi hop manner in order for communication process to take place [1]. The network is decentralized in nature where each node acts as router as well as host and does not need any access point for communication to take place. The main features of such a system is robustness, flexibility and mobility[1] due to which these systems play a major role in emergency and rescue operations and defense related operations [8].An Ad hoc network automatically establishes connection with the nodes present in networks , mostly ad hoc networks follow mesh topology. Ad hoc networks depending on the purpose they are deployed for can be further subdivided into three major categories these are MANET (mobile Adhoc Networks) an infrastructure less network of mobile nodes communicating through radio waves, VANET (Vehicular Ad hoc Networks) using cars as nodes for the flow of information to pass between them, WSN (Wireless Sensor Networks) consisting of autonomous sensors for controlling the environmental actions [1].

MANET as the name implies is the network of mobile nodes, mobile nodes includes portable devices such as laptops, mobile phones, smart phones etc which work by cooperating with each other in order for traffic flow to take place. [8][9] MANET are self organizing networks where each node is free to leave or enter a new network [3] MANET is the technology which enables communication to take place regardless of geographical location of the users [2]. Due to nodal mobility the topology of network changes anytime which makes it very difficult for message delivery to take place so for routing of message to the destination we require a routing protocol.

There are three types of routing protocol Reactive, Proactive and Hybrid Routing protocols [4]. Pro Active routing protocols are table driven routing protocols they maintain up to date routing information about each and every node present in the network and any changes in the network is reflected by sending updates in the network. Reactive or on demand routing protocol creates routes only when demand arises [4] a route discovery process is initiated after which a route is found it is stored in routing table eg: of reactive routing protocol is AODV (Ad hoc On Demand Distance Vector) routing protocol. Hybrid routing protocol combines the advantages of both reactive and proactive routing protocol. The routing is performed at two levels called inter zone and intra zone. If the forwarding and destination belongs to the same zone then route is established without any delay (proactive phenomenon) and else a route discovery process is initiated. As Proactive approach updates it a path too many times it depletes the network resources so reactive approach is more suitable as its more bandwidth efficient. AODV which is reactive routing protocol requests routes only when it's needed and saves lots of network resources. AODV uses control packets to initiate route discovery process and route maintenance. [5]When a node requires a route to a destination, it initiates a route discovery process within the network. A RREQ (Route request packet) is broadcasted in the network to the neighboring nodes which replies to the source node with RREP (Route Reply) creating a reverse path if they are the destination themselves or are having a fresh enough route to destination. Otherwise RREQ packets are rebroadcasted in the entire network unless and until a fresh enough route to the destination is found [5].

MANET networks operate in dynamic environment so authenticity of each and every node in the network cannot be deciphered which degrades the security mechanism of the system.[6] Attack taking place in MANET can be external or internal in the network mostly routing protocols become a target for attacker nodes. The routing attacks take place in network during route discovery or packet delivery. Some of the routing attacks are example Black hole attack .This attack occurs at Network Layer in which, a malicious node uses its routing protocol in order to advertise itself as having the highest sequence number and shortest path to the destination node or to the packet it wants to interrupt. The black hole node uses fake RREP packets and sends the reply to node first and ultimately drops the packets [6]. Gray hole attack which is denial of service attacks its sends true RREP for route requests but ultimately drops the packets of selective node and acts as normal nodes for remaining nodes. Worm Hole Attacks forms tunnel between true and malicious nodes and passes packets through the tunnel to malicious nodes and never delivers packets to the destination. Various works have been proposed till date which deals with these attacks .One of proposed mechanism to deal with black hole attack is concept of further RREP and further RREQ packets [6] .In this method in addition to sending RREQ to intermediate node further RREQ is send to the next hop of neighboring if it has route to destination and intermediate node it will send a further Reply to source otherwise not. So if a node is fabricating a fake response it can be easily identified but this method largely increases the overhead.[6]. To mitigate Worm hole attack two methods Watch dog method and Path Rater are used .Watch dog method identifies misbehaving nodes and path rater helps routing protocols to avoid these nodes.[10]Another scheme for dealing with Attacks is black hole resisting mechanism. In this technique a fake RREQ packets are send using fake source and destination if it receives reply to its fake RREQ then it indentifies the malicious node and isolates that node form the entire network.[7]

2. Black hole resisting mechanism Technique (BRM-AODV)

A Technique known as Black Hole Resisting mechanism makes use of trustiness table and black hole node list and also monitors the activities of neighbouring node for detection of Black hole attacks. . This protocol functions in the manner similar to normal AODV but uses the concept of Self Protocol Trustiness which makes malicious nodes to themselves give indications of their presence in the network. This Protocol does not make use of threshold values for Black hole detection but introduces modified control packets called fake RREQ which in its header information contains addresses of fake source and fake destination .As the Fake RREQ are broadcasted in the network the genuine neighbouring nodes do not recognize the destination address and do not have any route meant through them towards Destination in their routing table. So they do not reply to this control packet meant to detect the validity of neighbouring node. On the other hand the malicious or Black hole node does not check its routing table before replying and constructs a fake RREP with highest Sequence number and minimum number of hops and sends this message to the originator node. The source node on receiving this packet checks its trustiness table for the fake addresses of destination and source and if the value of addresses match then node becomes sure that the RREP has come from a malicious node so at this instant it does two steps [7]

1) Calculates the latency between RREQ packets and RREP packets by dividing it with number of hops the RREP packet takes to reach the originator. This gives the per hop time for latency between source and destination. The originator node already contains a table having time of last 3 hops of neighbouring nodes [7]
2) Sends an alert message to its neighbouring node for not to receive any RREP packets from this node whose address is calculated either from the source address presents in the packet or from the number of hops the packet takes to reach source.

Each node present in the network are assigned two variables called Trust variable and Confidence variable. In the dynamic environment nodes keeps on coming and leaving the network in a random manner so every new node joining the network is assigned a trust level of normal which changes according to the response of the node towards the fake RREQ packets .If it replies to the fake packet then trust level is changed to THREAT and if not then it upgrades its trust level to TRUST. The node changes its trust level from THREAT to NORMAL to TRUST if it does not receive RREP for consecutive two fake RREQs in RREP _VALIDATE period. In a similar manner nodes present in the neighbourhood are assigned confidence level which also increase or decreases depending on the response received .The confidence level of black hole node or colluding node is set as zero. If a node replies to the fake RREQ the originator node sets its value in the black list table as 1 and ignores all RREP received from this node. The fake RREQ are sent by the source at random time interval between MIN_NORMAL to MAX_NORMAL.

2.1 BRM-AODV Mechanism

a. Fake RREQ are sent at random interval between Min_NORMAL or MAX_NORMAL and in return if, a reply is received then there is possibility of threat from Black hole node or Colluding node.

b. Black hole node: These nodes itself constructs fake RREP packets and sends them to source advertising itself as having highest sequence number and minimum hop count and when receive data packets it simply starts dropping them or sends it to an unknown destination Colluding node: This node itself does not generate any fake RREP but helps the malicious node in forwarding the RREP packets towards source .The malicious node uses colluding node as a victim node for forwarding packets.

c. After receiving fake RREP the confidence level is decreased of neighboring node .The source node does not degrade the confidence level of neighbouring node (which helps in forwarding the packet from malicious node) to zero immediately. If some misbehavior is detected in the network it decreases the value of confidence level by some measure. This node starts monitoring the activity of the neighbour's .if a black hole node is found in the neighbor (i.e. RREP is received) it marks its value in the Black list table as 1, Remove it from the routing table and ignores all the packets received from malicious node

d. After receiving RREP for fake RREQ and identifying both source and destination address in e the trustiness table and the address of this reply is not identical to the address of forwarding neighbor The node drops this RREP and computes the latency between sending the corresponding RREQ and this RREP and then divide this value by the hop count received in this RREP to calculate the per hop time for the received RREP. Then, the node compares this value to the average hop time of all routes included in the routing table. Each route has three previously stored per hop time values. If the per hop time of the received RREP is less than the average per hop time of all stored routes in the routing table, the node decrements this neighbour confidence level for each received RREP of a fake RREQ .[7]

3. Proposed Scheme (CBRM-AODV)

The existing protocol detects the black hole attack in network but the overall overhead in the network is increased and also the above mechanism fails to deal with collaborative attacks. The proposed scheme used for dealing with black hole attack is CBRM AODV i.e. collaborative AODV protocol which uses the same concept as in BRM AODV of maintaining trustiness table and black list table and assigning confidence level and trust level to the nodes present in network in order to deal with malicious nodes. This scheme uses the concept of forwarding ratio which is the number of packets delivered by intermediate node. Using this forwarding ratio many attacks like gray hole, black hole and worm hole can be dealt with. Also the overall network parameter performances are much improved in comparison with BRM AODV protocol.

CBRM- AODV Algorithm:

```
Input: n number of nodes in the network.
1. Initialize the network
   for i=1:n
        a) N(i) trust level=Normal
        b) N(i)confidence = Max Confidence
        c) N(i)f(r)= 0.5 where f(r) is the forwarding
           ratio
    exit for
2. Select the source and destination
3. interval=Min_Normal
```

```
 t=0
4. Generate fake request from the source
5. Process RREQ using Normal AODV if n.mal=! 1
6. if source receives RREP from the node
    if n(i) level=normal
                n(i). Level= threat
                n(i).confidence=min_confidence
        elseif  n(i). Level=trust and n(i).fr=min and n(i).fr=max
                n(i).level=threat
                n(i).level=min_confidence
        else
                n(i).level=normal
                n(i).confidence=min_confidence
        endif
  elseif
        n(i).level=threat
        n(i).mal=1
 elseif
        n(i).fr=min or n(i).fr=max
        n(i)=! Trust
        n(i)=! Max_confidence
 endif
```

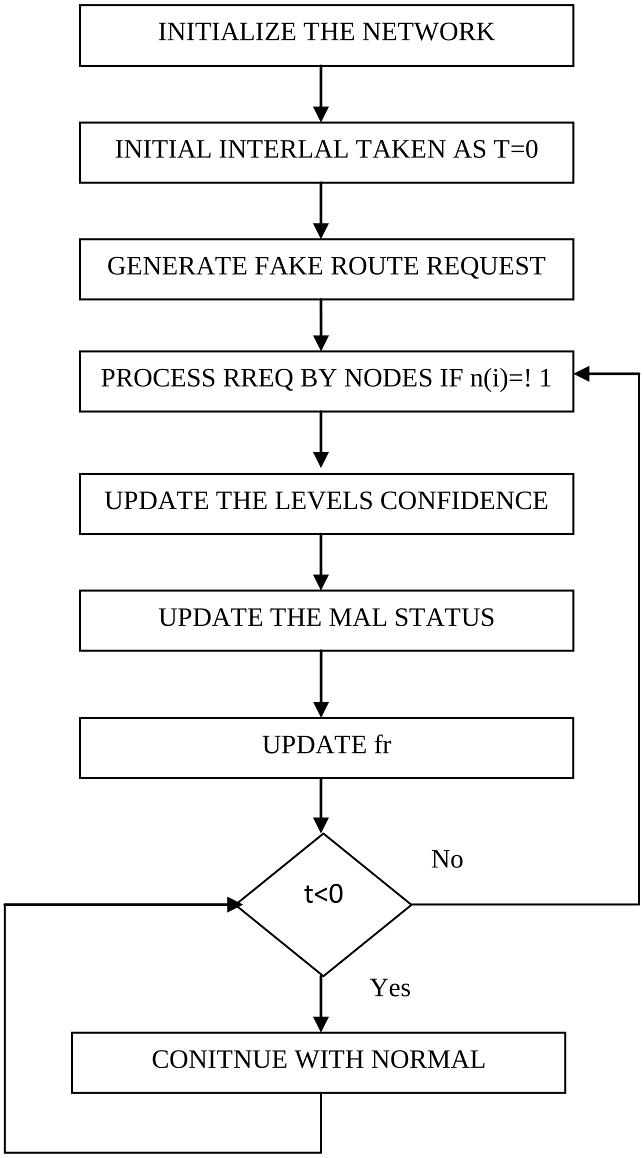
INITIALIZE THE NETWORK
INITIAL INTERLAL TAKEN AS T=0
GENERATE FAKE ROUTE REQUEST
PROCESS RREQ BY NODES IF n(i)=! 1
UPDATE THE LEVELS CONFIDENCE
UPDATE THE MAL STATUS
UPDATE fr
t<0
No
Yes
CONITNUE WITH NORMAL

Figure 1: Flowchart of CBRM-AODV

The implementation and analysis of result has been in next section.

4. Result and Discussion

The algorithms discussed in previous sections are implemented using NS2 and analyzed over different network having different number of nodes attacks. Various Parameters used for Analysis are packet delivery ratio, throughput, End to End Delay (E2E Delay), Overhead.

The following figures compare PDR of existing protocol with Proposed Protocol for 100 number of nodes

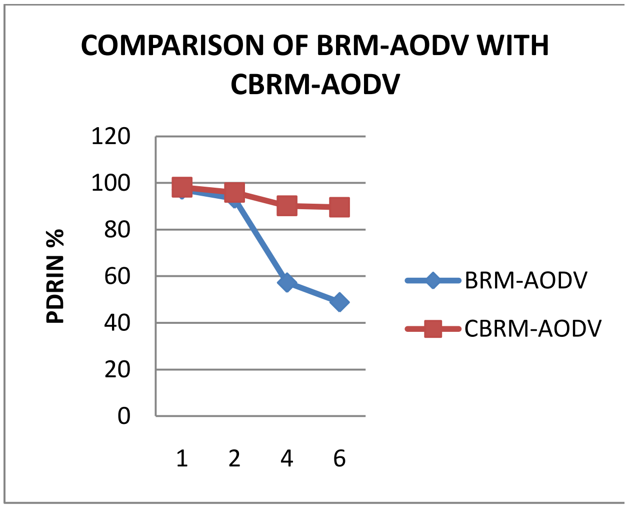

Figure 2: Comparison of PDR

For 100 nodes the packet delivery ratio of BRM AODV reaches a very low level while CBRM AODV protocol follows the same trend as was observed for lesser number of nodes or when malicious nodes were less . The graphical analysis shows that PDR for proposed protocol is very high as compared to the existing protocol and remains nearly constant even if we vary number of nodes or total number of malicious nodes in the network .its delivery remains fairly high and constant which leads to increase in performance of system. The following list of figures compares throughput of existing protocol with proposed protocols for different numbers of normal and malicious nodes:

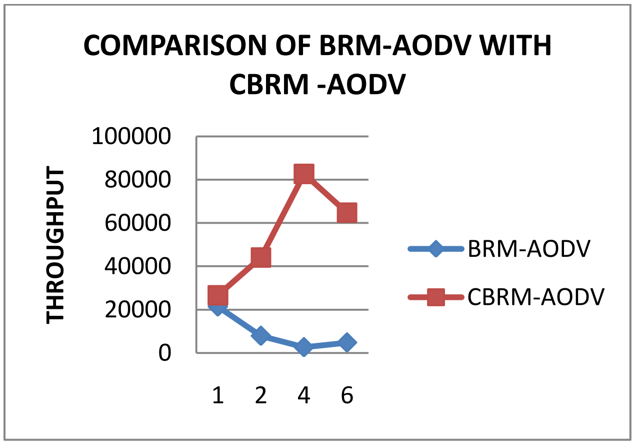

Figure 3: Comparison of Throughput

Comparison of existing protocol with proposed shows that CBRM AODV protocol is much more efficient in comparison with BRM-AODV as value of throughput remains fairly high in comparison with BRM AODV protocol. SO for performance enhancement of a network CBRM AODV is preferred.

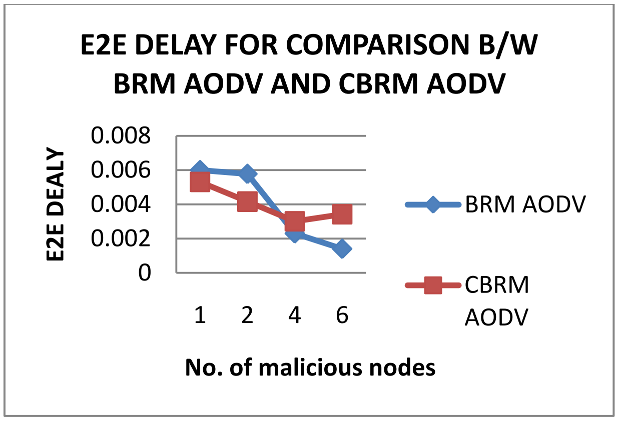

Figure 4: Comparison of E2Edelay

The conclusion that can be drawn from above list of graphs is that implementation of CBRM AODV allows least number of packets to be dropped in the network so when a malicious node is encountered in between source to destination it changes the route of packet transmission and in some cases the route followed is of longer length which sometimes increases the end to end delay in the network but delivery of packets at destination is guaranteed.

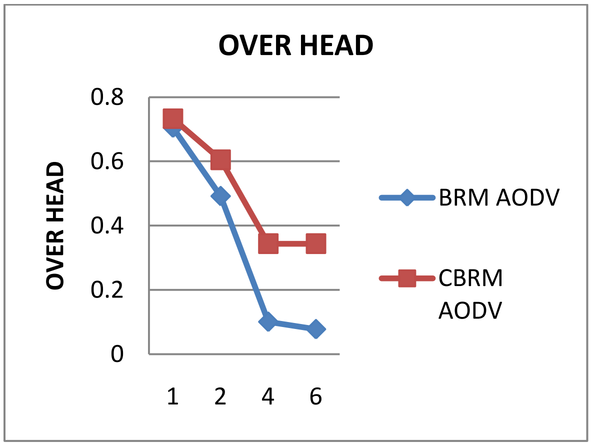

Figure 5: Comparison of Overhead

The value of overhead in CBRM AODV takes varying values for large number of nodes in the network and remains slightly higher than existing protocol due to which a little higher bandwidth is consumed for CBRM AODV protocol but overall performance of the network in terms of packet delivery ratio and throughput and end to end delay is enhanced .s o increased value of overhead does not affect the networks performance

5. Conclusion and Future Scope

The paper designs an algorithm to handle the collaborative and cooperative network layer attacks particularly blackhole, wormhole and grayhole attack. The paper uses the confidence level, trust level and forwarding ratio to check the reliability of the node. The results of the work on a network having 100 nodes show that the PDR and throughput has been improved while maintaining the e2edelay. This shows the significance of the work. In future the technique can be extended to work on other routing protocols.

References

[1] Helen, D., & Arivazhagan, D. (2014). Applications, advantages and challenges of ad hoc networks. JAIR, 2(8), 453-7.

[2] Bang, A. O., & Ramteke, P. L. (2013). MANET: history, challenges and applications. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(9), 249-251

[3] Bakshi, A., Sharma, A. K., & Mishra, A. (2013). Significance Of Mobile AD-HOC Networks (MANETS). International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2(4).

[4] Jadeja, Nehal, and Roma Patel. "Performance evaluation of aodv, dsdv and dsr routing protocols using ns-2 simulator." Performance Evaluation 3.2 (2013): 1825-1830.

[5] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[6] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. Communications Magazine, IEEE, 40(10), 70-75.

[7] Abdelshafy, M. A., & King, P. J. (2016, January). Resisting blackhole attacks on MANETs. In 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1048-1053). IEEE.

[8] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. An Overview of Mobile Ad Hoc Networks: Applications and Challenges.

[9] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.

[10] Kaur, Damandeep, and Parminder Singh. "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack." International Journal on Network Security 5.1 (2014): 62.