AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention Technique for Manets

Abdulaziz Aldaej
College of Computer Engineering & Sciences
Prince Sattam Bin Abdulaziz University

Tariq Ahamad
College of Computer Engineering & Sciences
Prince Sattam Bin Abdulaziz University

***Abstract*—Security is a major concern that needs to be addressed in Mobile Adhoc Networks because of its vulnerable feature that includes infrastructureless environment, dynamic topology, and randomized node movement making MANETs prone to various network attacks. Synergetic attacks have raucous effects on MANETs as compared to particular single attack. Various algorithms and protocols have been designed and developed to meet the increasing demand of MANET security but there is still a room for improvement in order to make it more reliable and hassle-free communication. An AggrandizedAODV is presented in this paper to detect and prevent various synergistic and non-synergistic attacks.**

Keywords—MANET; AODV; Grayhole; Blackhole

I. Introduction

MANETs or Mobile Ad hoc Networks are arrangement of non-stationary nodes communicating with each other without any prevailing network infrastructure hence nodes are autonomous i.e. each node acts as source, destination and as router themselves as par need [1]. Nodes or devices enjoy the freedom to move in any direction any time, these nodes inhibit self-configuring or adaptive, self-healing, peer to peer characteristics made possible with introduction of routable network capabilities on the top of Link layer [2]. MANETs flexible mode of operation, least communication infrastructure requirement, adaptability to continually changing scenarios or topologies, operability in low computing capacity, connectivity in scarce bandwidth and communication without any centrally controlled entity provide them special significance in the conditions where making network infrastructure is infeasible or impossible [3].

Because of their special characteristics MANETs have different set of communication protocols especially suited for their needs. Broadly MANET routing protocols can be classified into three categories viz. Reactive Protocols, Proactive Protocols and Hybrid Protocols. Reactive Protocols do not initiate route discovery on themselves unless requested by any node to do so [4]. Their more common name ‘On-Demand’ originate from fact they find route to certain destination node when demanded, Hence don’t consume precious bandwidth of MANETs, These protocol start route discovery with flooding RREQ, destined node or any intermediate node having route information for requested node can send back route information with RREP. Once route becomes active route node keep track of changes, if any intermediate or destination route moves or goes offline subsequently a RERR is generated to inform neighboring node about link break [5]. Most prominent protocols of this category are Dynamic Source Routing (DSR) and Ad hoc On Demand Vector (AODV) protocols.

Another way around for routing is Proactive Protocols which alike their wired counterparts maintain a routing table and update it regularly for any network changes. Every single node is known to every other node of the network i.e. each node in network has route information about other nodes of the network. In case of any change in network topology all nodes update their routing table to reflect this change [6]. Optimized Link State Routing (OLSR) protocol falls under this category.

As usual, all of these protocols have pros and cons associated with them which vary on routing overheads, throughput and memory overheads etc. none of them is ideal for all situation, although various variation of them have been proposed, researched and tested still wide scope of improvement in detection and defense of MANETs against wide variety of attacks exists. Each protocol has its own issues associated with them.

A compromising solution obtained with combining strengths of these two categories is Hybrid Protocols. MANET is divided into parts or zones, portion of which follows reactive protocols and portion is maintained by proactive protocols [7]. An example of which is Zone Routing Protocol (ZRP) it incorporates proactive protocols for route setup inside zones whereas utilizes reactive protocols for inter zones route setup. A node may have overlapping zones of different routing pattern [8].

Irrespective of routing protocol used security remained a prime concern of MANETs. MANETs are highly prone to a series of attacks exploiting range of features inherent with MANETs, from flexibility to enter and exit from network to scalability attacker had exploited each characteristics of network which distinguish it as MANET [9]. Out of various attack our study is focused upon DoS attacked camouflaged as Black hole attack where a node deliberately drops all packets and keep on sending route message lucrative enough as shortest route in some cases, coordinated black hole attack where more than one compromised node work in tandem to launch Black hole attack and gray hole as special case of black hole attacks where node selectively drops some packets and forward some packets making it more difficult to detect and isolate [10].

II. RELATED WORK

A number of researchers have studied Threat of collaborative attacks on MANETs in recent past, defending mechanism; preventive approaches have been taken on extensively.

In [11] each node incorporated a DRI or Data Routing Table and methods to cross validate it for detecting cooperative black hole nodes in the network. This mechanism was embedded into modified AODV routing protocol. Experimentally it was found this method out performs other proposed solutions.

In [12] author demonstrates some of the frequent attack mechanism and eventually analyses possible collaboration among various attacking entities. Author further tries to evaluate various machine learning techniques viz. DSP (Digital Signal Processing) and ANN (Artificial Neural Networks) in detection and prevention of collaborative attacks in MANETs. Their analysis showed collaborative attack in wireless network is much more devastating and crippling effects than wired one. They also experimentally insinuated effectiveness of the model framed to minimize collaborative attack and immunizing the mobile ad hoc networks.

In [13] the problem of collaborative attack with in from the network was discussed where critical data inside the Information System is at risk from two or more malicious nodes working in some accord. In this proposed approach, authors begins with mutual relation of different illegal information flow diagrams and components of information systems. Later on, he classified and summarized data access patterns on the basis of mutual-access-record's probability value and transaction distance of data items, ultimately proposed an algorithm for early detection of collaborative insider attacks.

In [14] authors have carried out a detailed analysis of MANETs under single and collaborative Black Hole Attacks and based on their analytical finding proposed mechanism to prevent attack by rerouting network traffic to avoid Black Hole nodes. Proposed MANETs utilizes AODV protocol for its robust features, proposed mechanism rely on transmitting only confirmation packets which have been verified by the destination for the presence of black hole in the GAODV routing Protocol.

In [15] the author forwarded a theory that balanced collaborative attackers can eventually by pass security measures imposed by trusted node assistance methods which are readily used in available security setups. Based upon their theoretical findings, Balanced Collaborative attackers can be seen with highest similarity ratios. Authors forwarded an algorithm to find anomalous behavior of nodes and early detection of balanced collaborative attackers. The only information required for knowledge of reporting channel is bit error probability of secondary users. Simulation results depict efficiency of proposed technique in identification of balanced collaborative attackers. Paper proposes a novel technique for detection and subsequently prevention of collaborative attacks in MANETs focused on detecting and isolating malicious nodes through bridge data items.

III. PROPOSED AAODV (AGGRANDIZED AD HOC ON DEMAND VECTOR)

Two interdependent control packets can be used to enhance and improve the existing AODV.; SRRD_REQ and SRRD_REP. their function is same as that of RREQ and RREP but more reliable and with more steps. SRRD_REQ message along with associated SRRD_ID are sent by the source node as destination node's DSN over the MANETon equal continuous intervals and after evaluating the authentic SRRD_ID, SRRD_REP packet is sent as response to the SRRD_REQ node by the destination node and generates SRRD_REP only to notify that no other node is needed other than destination node and can generate SRRD_REP. in addition to this, threshold vale (TV) and Reliability list are added to routing table as new fields. Addition of these two fields doesn't mean that there is going to be any change in the AAODV routing table as compared to AODV routing table but just a couple of more fields.

The reliable list field contains the list of trust worthy and reliable nodes and TV fields contains the DSN average of trustworthy nodes. Following are the two major steps that are used in route discovery.

AAODV Algorithm

The AAODV to detect and defend MANET from attacks is explained in two phases.

Phase I.

Whenever a MANET node wants to communicate with other nodes in the nwtwork the first thing to do is to check if an updated route is present in the routing table. Forward the data packet in case there is a reliable route otherwise start the route discovery procedure that involves sending SRRD_REQ by the source node to their 1-hop nodes with associated SRRD_ID to create a new route. Following are the steps followed by the immediate node after receiving as SRRD_REQ.

1) Send reply to the requesting node and SRRD_REP if an updated route is present otherwise forward this request to the first hop nodes.

2) Set up a reverse route discovery for the REP messages.

3) If the node is possess an outdated routing table entry as destination it refreshes it and if RL contains an entry for destination node then erase and update the entry.

4) If there is no entryfor the source in the routing table then using RPT create a new entry and in case of various available reliable routes, arrange them in the order of their hop count. After going through all these steps compare the top reliable routes of first node on the basis of DSN having least hop count with TV. In case its value is higher than the route nodes DSNs average then discard this route as it is a malicious node and keep checking until reliable route is found with less DSN value as compared to TV.

5) The source nodes new entry is selected as most reliable route having least hop counts involves hop count, SRRD_REQ sequence number and address of the node which responded first to the broadcasted request packet acts as next hop.

After receiving the SRRD_REQ from the source, the destination node uses reverse path to send SRRD_REP. sometimes an intermediate node with a reliable updated route the destination also sends SRRD_REP. thus during RRT every node must perform the following tasks after receiving the SRRD_REP.

1) If the node contains an outdated route entry for the destination node then it must update the entry otherwise create a new routing table entry.

2) IP address of the source node must be added to the entry and can be copied from SRRD_REP packets originators field. Forward_Data_Packet_Counter and SRRD_ID both are assigned zero and forward it to next node on reverse path.

In normal AODV route discovery procedure is executed when source node receives RREP but in AAODV one more procedure gets invoked from this stage onwards.

Phase 1 Code.

```
Input:  SRRD_REQ(), reqNode,destNode,relNodeList[],
hopCount , maxHopCount, routeDiscovery(), selRoute(),
sendPckt()

Begin
    SRRD_REQ()
    if (reqNodeϵ relNodeList[]) Truethen
        selRoute()
        sendPckt()
        stop
    else
    routeDiscovery()
    if (SRRD_REQ ← destNode) False
        if (hopCount>= maxHopCount) True
        stop
        elseSRRD_REQ()
        end if
    else
        routeForm()
    end if
end
```

Phase II

The source floods route requests towards every neighbor node and then sends SRRD packets to all those who responded with RREP (route replies). Following are the steps for that every nodes that received SRRD packets.

1) If routing table contains an entry for reverse path, it sets or initializes SRRD_ID by imitating that from SRRD otherwise a new entry is created by the node.

2) Will send packets to that every node which replied with SRRD_REP earlier.

3) Every node must have an entry for the destination that is on the path of SRRD.

The SRRD_REP is sent to hop node that responded first with an SRRD packet and ignores the rest after receiving SRRD packet by the destination. Reliability value is set to one (1) in the SRRD_REP packet by the destination. During RPT every first hop node receives SRRD_REP once only (SRRD_ID=1) for the first time and in SRRD_REP assigns 0 to Forward_Data_Packet_Counter and using reverse path forwards it to next node and a unique SRRD_REP is received by the source and a reliable route is discovered and no node can generate any SRRD_REP at all.

Phase II Code

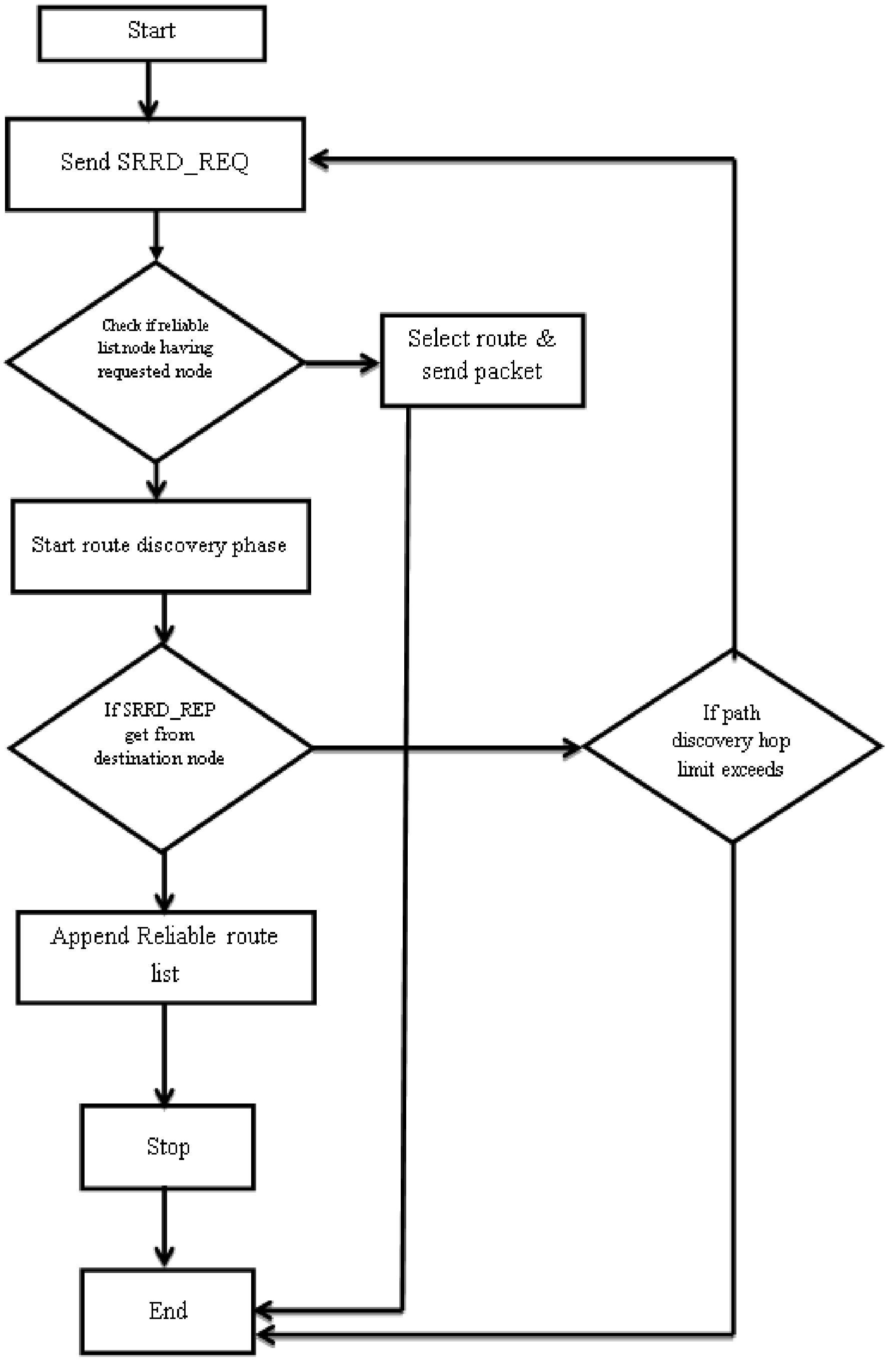
```
Input: relRoute(), sortRoute(),
RevrsTrace(), hopCount, sendPckt(),
rejectRoute

Begin
    relRoute()
    sortRoute(hopCount)
    RevrsTrace(source ← dest)
if ( DSN > TV) True then  ▷ for first
node at each intermediate node
    rejectRoute ← True
    stop
```

```
else
    Procedure selRoute(minHop)
    Procedure Update(route &relList)
```

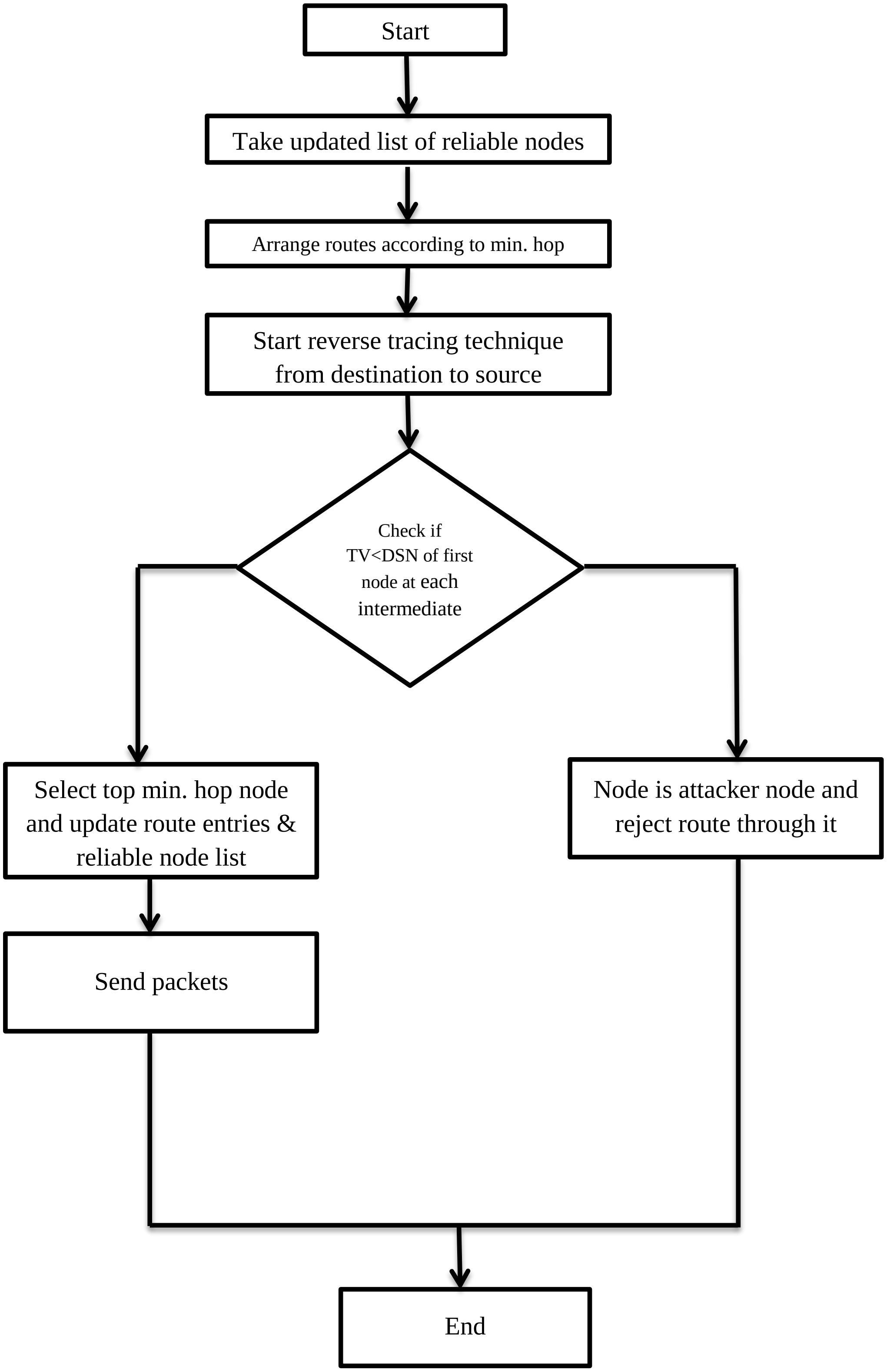
```
    sendPckt()
end if
end
```

Flowchart of AAODV

PHASE 1


Start
Send SRRD_REQ
Check if reliable list node having requested node
Select route & send packet
Start route discovery phase
If SRRD_REP get from destination node
If path discovery hop limit exceeds
Append Reliable route list
Stop
End

Flowchart describing Phase 1 of AADOV


Start
Take updated list of reliable nodes
Arrange routes according to min. hop
Start reverse tracing technique from destination to source
Check if TV<DSN of first node at each intermediate
Select top min. hop node and update route entries & reliable node list
Node is attacker node and reject route through it
Send packets
End

PHASE II

Flowchart describing Phase 2 of AADOV

Simulation and Result

A MANET scenario is designed for the simulation and predefined parameters of the simulator and the necessary attributes of the nodes are configured. We have used NS2 for simulation in this network model. The complete network model is designed using some values and they will be crucial in providing us with more accurate simulation results as compared to results before this one. Following is the table containing parameters and their values used for simulation.

TABLE I. PARAMETER AND INITIAL VALUES OF THE EXPERIMENT

Parameter	Value
Total Number of Mobile Nodes	25
Total number of Static nodes	4
Total number of Base Station nodes	1
Total number of Black hole nodes	3
Total number of Gray hole nodes	2
Routing Protocol	AODV
Attack Protocols	Black hole AODV,
	Gray hole AODV
Simulation Time	90 Seconds
Data Rate	10KBPS
Regular Msg Size	512 b
Irregular Msg Size	1024 b
Traffic	CBR

A network with 25 nodes is generated using NS2 allowing some nodes to act as black hole and gray hole like a normal scenario in AODV. Source and destination connection in this MANET is done by UDP and a constant packet traffic is generated through the UDP using CBR application. CBR packet size and data rate is set to 512 bytes and 1024 bytes respectively. And this same procedure with same settings, values, connection methodology and traffic generation is used for AAODV.

In figure 1, we observed thoroughly that the normal AODV got affected radically by blackhole and grayhole nodes and gets increased when the number of malicious nodes increases. This acknowledges the fact there is not enough secure technique to detect and prevent blackhole attacks or grayhole attacks using normal AODV. Our proposed AAODV provided better and higher packet delivery ratio as compared to normal AODV in all the conditions (like no attack condition, with black hole only, with blackhole and gray hole together). We also set the number of malicious node in the MANET ≈ 50%, AAODV still provided us better results as shown in the figure 1 in detecting and preventing from malicious nodes successfully even after we kept the packet delivery ration more than 75%.

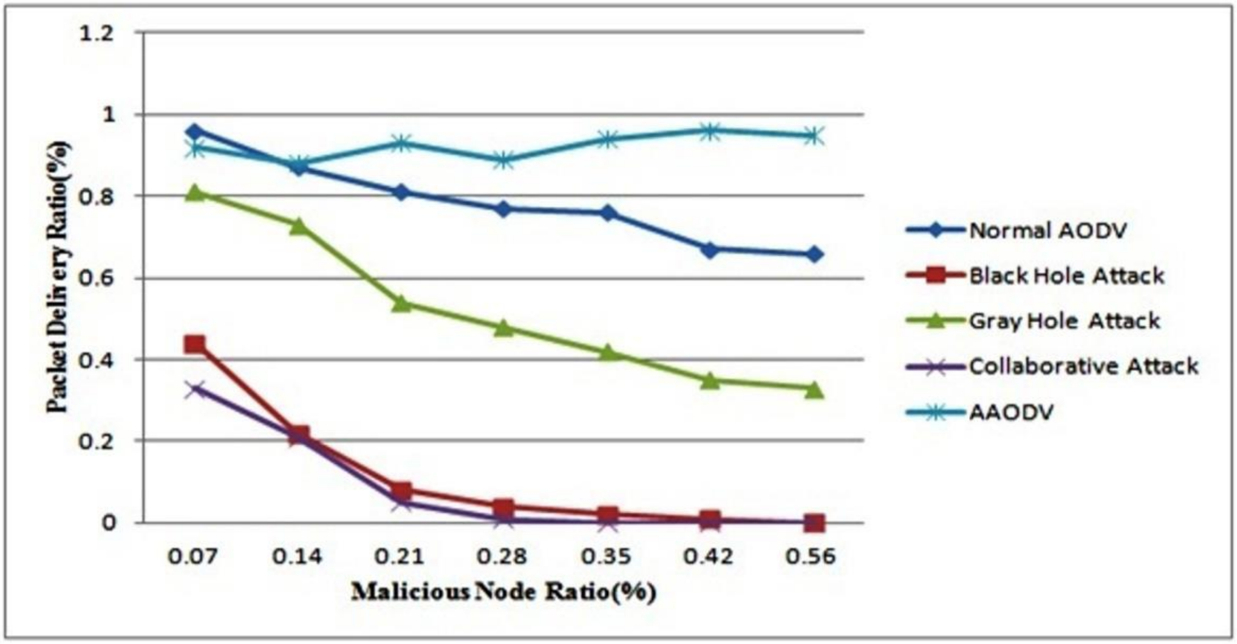


Fig. 1. Packet Delivery Ration of AODV and AAODV in different situations

In figure 2. Keeping malicious node ratio as benchmark, we did a thorough study of AODV's and AAODV's routing overhead and gained result proved that when the number of black hole and Grayhole nodes is increased the proposed AAODV produces better routing overhead AODV. Thus proving the fact that the existing normal AODV doesn’t possess a safe and reliable scheme to detect and defend the Blackhole and gray hole attacks. While the suggested AAODV proves better than the existing one.

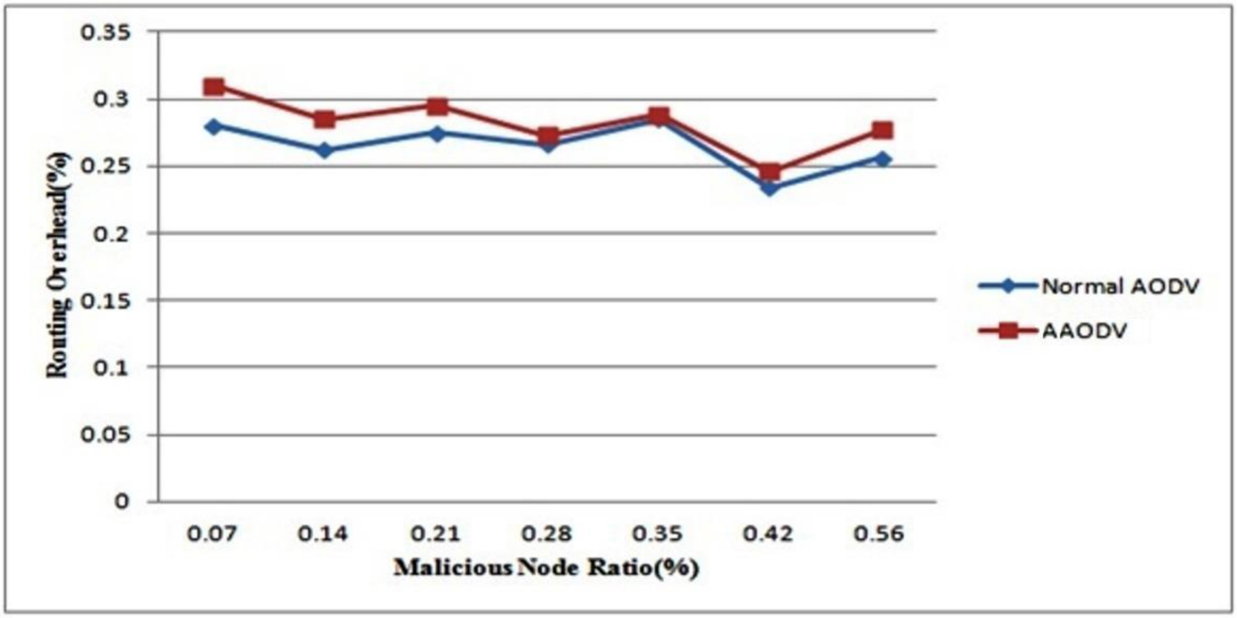


Fig. 2. Routing Overhead of AAODV and AODV

In figure 3. Average end-to-end delay of AAODV and AODV is used to generate the result putting MNR as measurement parameter. Output result graph shows that proposed AAODV attains better end-to-end delay average than the existing AODV. The result graph also shows that AAODV requires extra time to identify the malicious nodes.

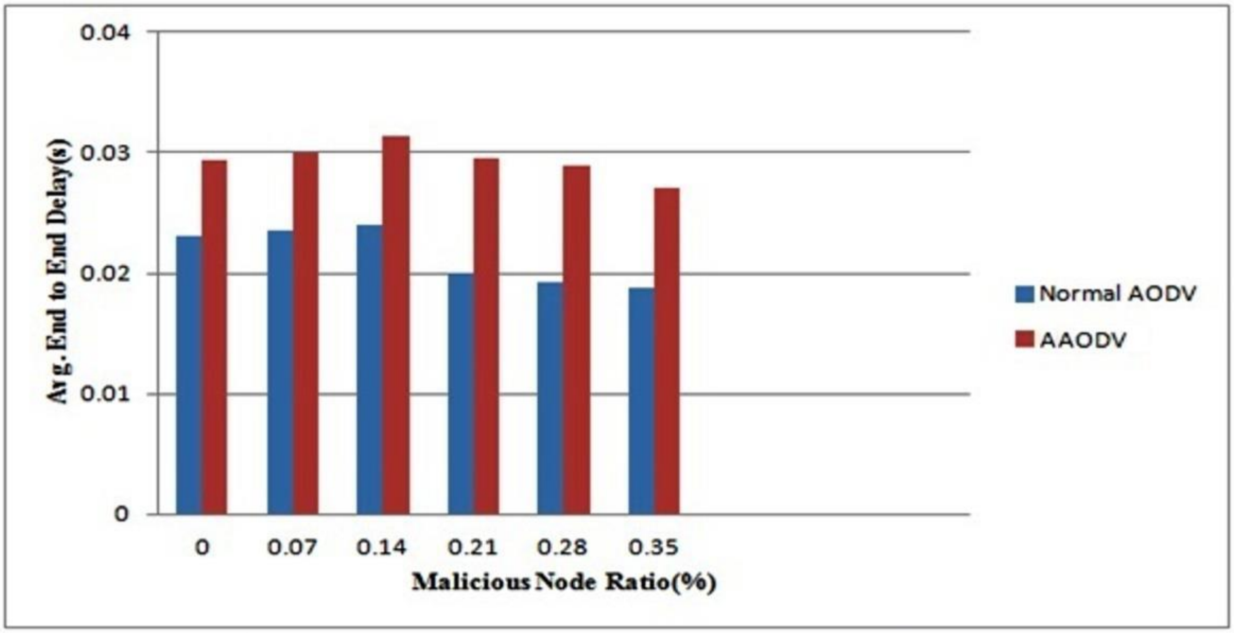


Fig. 3. Average of end-to-end delay in AODV and AAODV

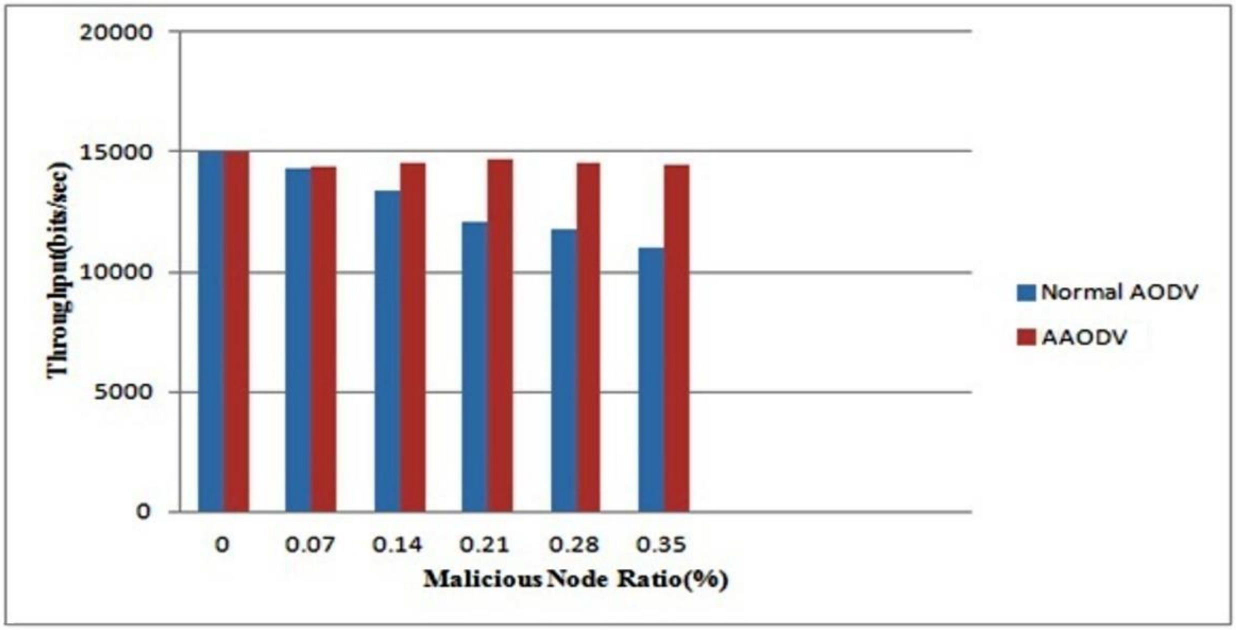


Fig. 4. Throughput of AODV and AAODV

In figure 4, after analyzing the throughput of suggested AAODV and the existing AODV putting MNR as measuring parameter , the result proves that the existing AODV got more Blackhole and gray hole attacks as compared to AAODV. During a scenario in which the number of Grayhole and Blackhole nodes in the MANET is higher (≥ 40%) the proposed AAODV can still identify the malicious nodes even if the throughput is higher than 14000 b/s.

IV. Conclusion

In this research article , we have proposed a AAODV (Aggrandized Ad Hoc On demand Vector) to detect and defend MANETs from malicious nodes during synergistic and single attacks like black hole and gray hole attacks. The proposed AAODV has proven to produce better results as compared to existing AODV protocol as the experimental simulation output graphs of packet deliver ratio, throughput and routing overhead shows improved results. The proposed technique is best appropriate for a MANET up to 50 nodes for detection and prevention from Grayhole attacks and black hole attacks. A minor routing overhead in suggested AAODV that averts the complete efficient application of MANET that is not the case with AODV. This increase in the size of MANET will increase the routing overhead. In future, the simulation can be enhanced to improve this AAODV to overcome this and to tackle with other amalgamation of attacks that can work together to target the MANET.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016/2017 under research number 2016/01/5693.

References

[1] Ahamad T, Aljumah A. "Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology. 2015 Dec Vol 8(33).

[2] Aljumah A, " Detecting Distributed Denial Of Service (Ddos) Attack Using TTLv Constraint In Mobile Adhoc Networks (MANET) ", Science Internationals, 2015 Dec Vol 27(6),5037-5040.

[3] Ahamad T, Aljumah A. ,"Ad Hoc Network & Black Hole - Threat and Solution". American Journal of Scientific Research , Issue 104 , Nov, 2014.

[4] Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.

[5] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and D. Gaiti, "Denial of Service (DoS) attacks detection in MANETs through statistical models," *2014 Global Information Infrastructure and Networking Symposium (GIIS)*, Montreal, QC, 2014, pp. 1-3. doi: 10.1109/GIIS.2014.6934261

[6] Tsou PC, Chang JM, Lin YH, Chao HC, Chen JL. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 13th International Conference on Advanced Communication Technology: Seoul; 2011 Feb 13-16. p. 755–60.

[7] Baadache A, Belmehdi A. Avoiding black hole and cooperative black hole attacks in Wireless Ad hoc Networks, International Journal of Computer Science and Information Security. 2010; 7(1):10–6.

[8] Arunmozhi S.A., Venkataramani Y."A Flow Monitoring Scheme to Defend Reduction-of- Quality (RoQ) Attacks in Mobile Ad-hoc Networks", Information Security Journal: A Global Perspective, Vol.19, No.5, 2010, pp.263- 272.

[9] Hyojin K, Ramachandra B. C., JooSeok S,"Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010, pp. 579-582.

[10] Mistry N, Jinwala D. C., Zaveri M,"Improving AODV Protocol against Blackhole Attacks", Proceedings of the International Multiconference of Engineers and Computer Scientist, Hong Kong, Vol. II, 2010.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks”, International Conference on Wireless Networks (ICWN), 2003.p.1-7.

[12] Tao Gong1 and Bharat Bhargava, “Immunizing mobile ad-hoc networks against collaborative attacks using cooperative immune model”, article published in Wiley Online Library (wileyonlinelibrary.com), Issue: Security and Communication Networks, 2013.p.58-68.

[13] Khanh Viet, Brajendra Panda, Yi Hu Korea, “Detecting Collaborative Insider Attacks in Information Systems”, IEEE International Conference on Systems, Man, and Cybernetics, Seoul; 2012.p.502-507.

[14] Sanjay K. Dhurandher, I. Woungang, R. Mathur, P. Khurana, “GAODV: A Modified AODV against single and collaborative Blackhole attacks in MANETs”, IEEE 27th International Conference on AINA Workshops, Barcelona; 2013.p.357-362.

[15] Mingchen Wang, Bin Liu and Chi Zhang “Detection of Collaborative SSDF Attacks using Abnormality Detection Algorithm in Cognitive Radio Networks”, IEEE International Conference on Communications, Budapest; 2013.p.342 – 346.