COMPARATIVE REVIEW STUDY OF SECURITY OF ARAN AND AODV ROUTING PROTOCOLS IN MANETS

Er. Ruby Goel[1], Er. Meenakshi Mittal[2]

[1]Computer Science and Technology, Central University of Punjab, Punjab, India
[2]Computer Science and Technology, Central University of Punjab, Punjab, India

Abstract

Mobile Ad-hoc networks are proposed because there are some areas where it is not possible to set up a network having fixed infrastructure, like in areas of emergency services, military operations, personal area networks, etc. Ad hoc network allows communication between wireless nodes with the help of their transmission ranges and routing protocols facilitate this communication among the nodes. But on these routing protocols variety of attacks are possible like- Eavesdropping, IP-spoofing, Blackhole, Denial of service attack, etc. By attacking the routing protocol attackers can access network traffic, can drop it or can modify it. To prevent these attacks many secure routing protocols like- SEAD, ARAN, SAODV, SRP, etc have been developed. In this paper security aspects of ARAN (Authenticated Routing for Adhoc Network routing protocol) has been analyzed with respect to a commonly used routing protocol AODV (Adhoc On-Demand Distance Vector) i.e. how much these two protocols are resistant to Blackhole and IP-Spoofing attack under GloMoSim-2.03 simulator.

Keywords: *AODV, ARAN, Blackhole, IP-Spoofing, GloMoSim.*

---***---

1. INTRODUCTION

In Ad-hoc networks the wireless nodes communicate with each other by forwarding packets over themselves. Mobile Ad hoc NETwork (MANET) is a network of mobile nodes that uses each other services to forward a packet to its destination. MANETS have several advantages over traditional wired networks as they are easy to deploy in a short interval of time and are independent of fixed infrastructure. Nodes in MANET can behave differently in the network as at one time a node can behave as a sender; other time as the receiver and can also help to route the packets to another nodes functioning as the router [9]. Nodes communicate to each other with the help of their transmission ranges and routing protocols defines the rules for communication. As discussed in [7], [9] these protocols come under different categories like-

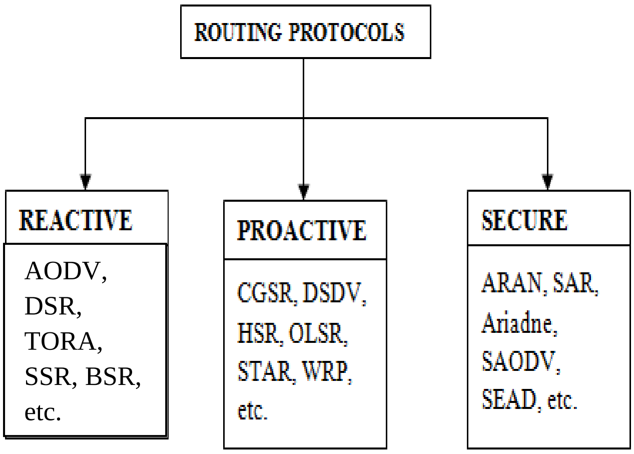
ROUTING PROTOCOLS
REACTIVE
AODV, DSR, TORA, SSR, BSR, etc.
PROACTIVE
CGSR, DSDV, HSR, OLSR, STAR, WRP, etc.
SECURE
ARAN, SAR, Ariadne, SAODV, SEAD, etc.

Fig –1: Various types of Routing Protocols

- **Reactive or on-demand**- here routes are only generated when they are needed by any source node to send the packets to another node.
- **Proactive or table driven**- here routes to all destinations are kept in tables which are regularly updated with changes in topology.

Reactive protocols found to be more efficient than proactive protocols because they use lower bandwidth for maintaining routing tables, and they are more energy-efficient and have effective route maintenance [9]. As discussed in [7] MANETs are subject to various security challenges due to:

1. Vulnerabilities of topology which is changing dynamically.
2. Absence of security infrastructures on wireless links.
3. Selfish behavior of nodes which may not participate in routing process genuinely.

Due to these reasons Reactive and Proactive protocols are subject to various attacks like- IP Spoofing, Blackhole, Eavesdropping, Traffic Analysis, Denial of service, etc.

- Secure protocols- To provide security features against above mentioned challenges secure protocols have been developed which are effective against various network attacks.

In [14], [15] AODV and ARAN performance had been compared on the basis of various metrics. In this paper ARAN performance has been checked against AODV under Blackhole attack and IP Spoofing attack.

The organization of paper is done as follows: Section 2 describes the two routing protocols AODV and ARAN.

Section 3 describes the Blackhole and IP-Spoofing attack. Section 4 describes the simulation setup and various simulations results. Finally, Section 5 concludes the paper.

2. ROUTING PROTOCOLS OVERVIEW

2.1 AODV (Adhoc on Demand Distance Vector) Routing Protocol [20]

Zhou in [20] has described that AODV is a pure on-demand routing protocol where routes are built only when nodes want to communicate or transmit data to other nodes. AODV functionality is described under two important procedures:

2.1.1 Route Discovery Procedure

Route request (RREQ) and Route reply (RREP) packets in AODV use various parameters like- s_seq (source sequence number), d_seq (destination sequence number), hop_count (number of nodes the message has passed), s_addr (source address) and d_addr (destination address) to find out the shortest route. AODV working is shown in Fig -2 where S (source node) wants to send data to D (destination node). S node broadcasts the RREQ packet to all neighboring nodes which will further broadcasts the packet until the destination is reached. After all the RREQ packets reach the destination node D, it unicasts the RREP packet upon the path with shortest hop count. So the RREP packet is sent through node I3 and being the shortest route S-I3-D path is selected.

2.1.2 Route Maintenance Procedure

If some link is found to be broken, route error (RERR) packet is sent to all the source nodes using that link. Thus route maintenance is done through RERR packets. As shown in Fig -3 node I1 sends Route error (RERR) message to source node S for the broken link. It consists of D_addr, D_seq and hop_count equal to infinity [17].

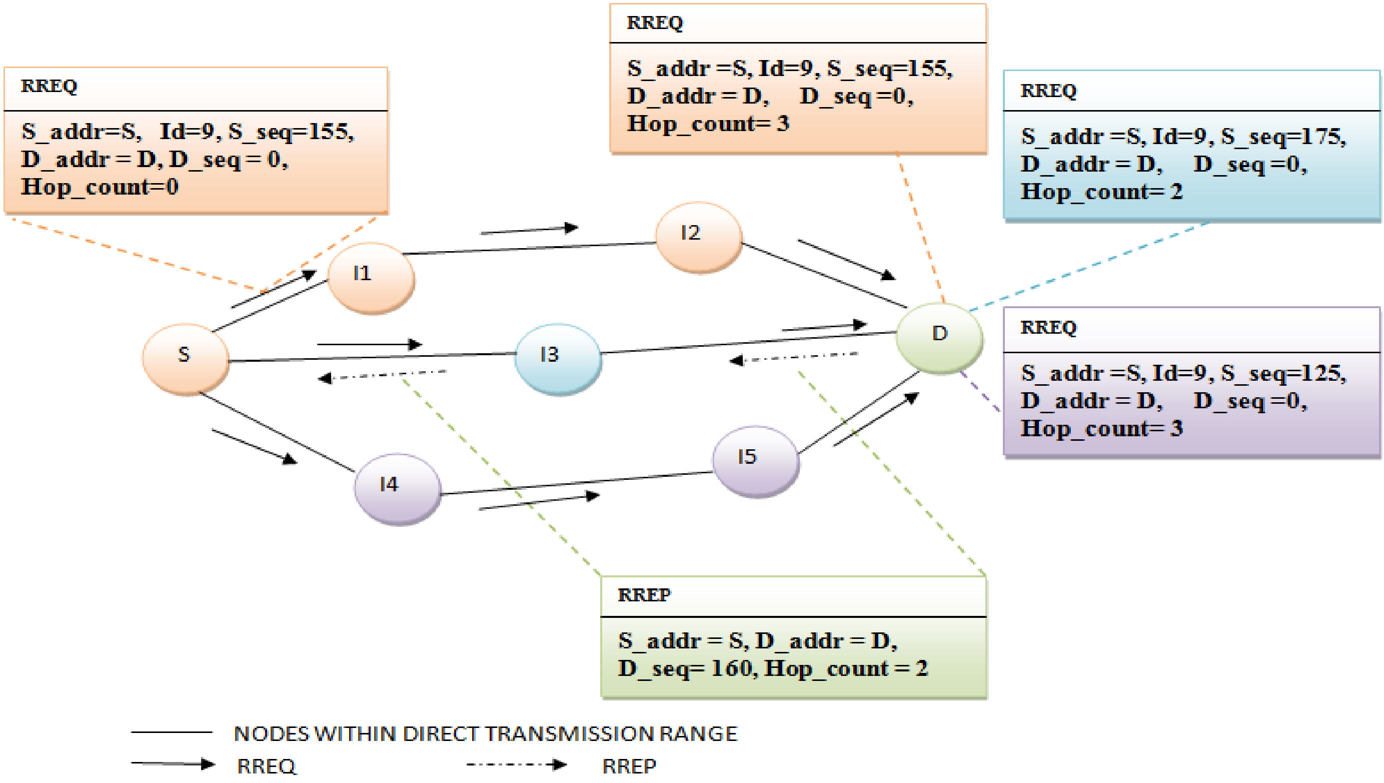

Fig -2: Route discovery process in AODV

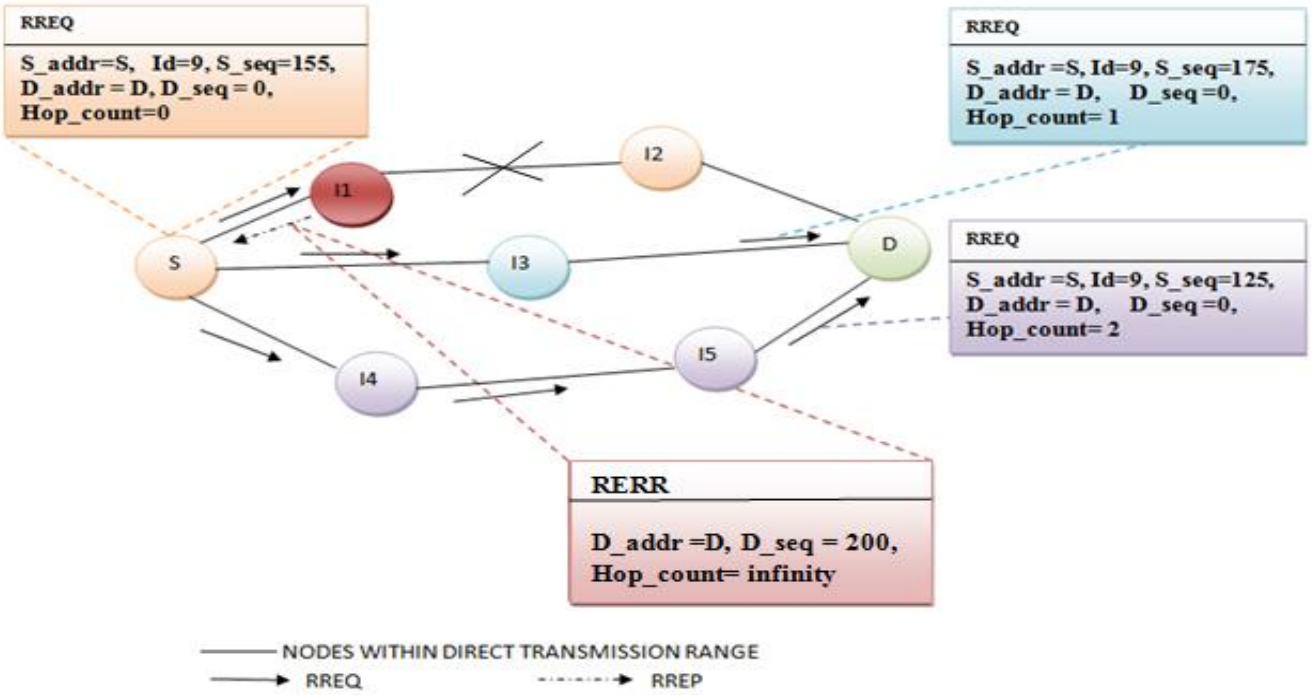
RREQ
S_addr=S, Id=9, S_seq=155, D_addr = D, D_seq = 0, Hop_count=0
RREQ
S_addr =S, Id=9, S_seq=175, D_addr = D, D_seq =0, Hop_count= 1
RREQ
S_addr =S, Id=9, S_seq=125, D_addr = D, D_seq =0, Hop_count= 2
I1
I2
S
I3
D
I5
I4
RERR
D_addr =D, D_seq = 200, Hop_count= infinity
NODES WITHIN DIRECT TRANSMISSION RANGE
RREQ
RREP

Fig -3: Route maintenance process in AODV

2.2 ARAN (Authenticated Routing for Adhoc Network) Routing Protocol [14], [15]

Sanzgiri, LaFlamme, Dahill, Levine, Shields, & Belding-Royer in [14], [15] proposed a secure routing protocol ARAN. ARAN provides security against third party attacks by introducing authentication, message integrity and non-repudiation. Every node in ARAN has a certificate from a trusted server; so that no illegal node can participate in routing process. ARAN protocol consist four steps: Certificate application, route discovery, route establishment, route maintenance. ARAN doesn't record the entire route information and also doesn't consider the total number of hops in the route discovery. Each legitimate node only records the IP address of its precursor nodes and successor nodes. This ensures the security of the network topology that no unauthorized node can participate in routing process. ARAN functions by verifying the signatures of its predecessor node before accepting the RREQ packet or the RREP packet. As shown in Fig -4 node I1 verifies the signature of node S; I2 of I1; I3 of I2 and D of I3 while sending RREQ packet and I3 verifies D node signature; I2 of I3; I1 of I2 and S of I1 while receiving RREP packet. Finally after all the verification a route is established between S and D [14], [15].

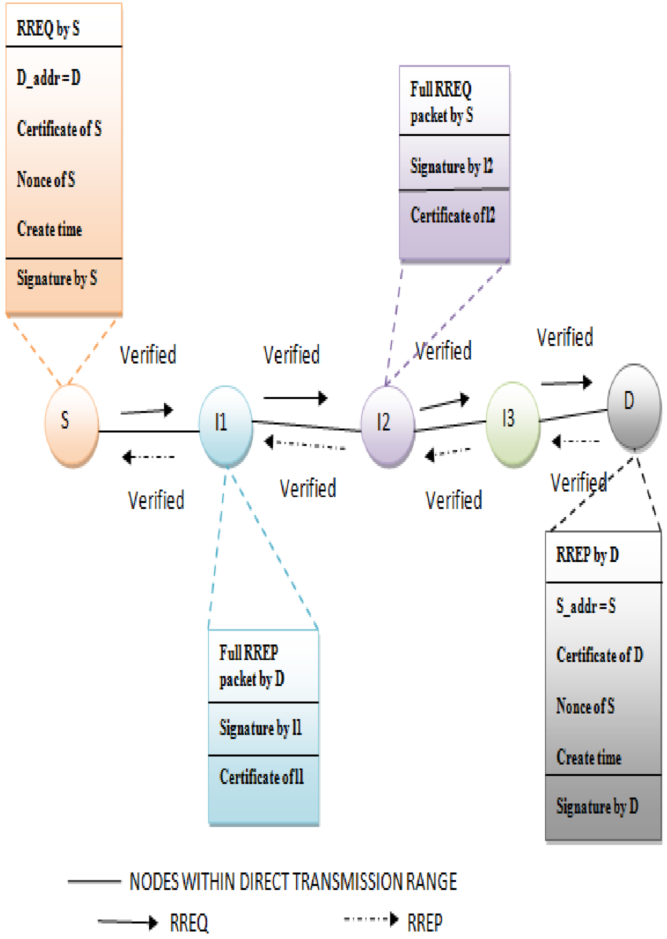

Fig -4: Route discovery in ARAN

2.3 AODV vs. ARAN

Both the protocols can be compared on the security basis as shown in Table –1.

Table –1: Attacks possible in AODV and ARAN [14]

Attacks	AODV		ARAN	
	YES /NO	REASON	YES /NO	REASON
Blackhole	YES	Hop count and Sequence number can be easily modified	NO	Hop count and Sequence number does not exist
Message Modification	YES	No check on message contents	NO	Digital signature by the sender prevents modification in message content
IP- Spoofing	YES	Source address is not verified	NO	Source address is verified by sender's digital signature
False Route Errors	YES	Can be sent by any node by using IP-spoofing	YES	Can be sent by any node but sending node can be detected by digital signature and certificate
DOS or DDOS	YES	Congestion can be created by using IP-spoofing	YES	Congestion can be created by legitimate nodes

Table –I shows that though ARAN prevents many attacks but denial-of-service attack can be conducted by nodes having or may not having valid ARAN certificates [14], [15]. If a packet is routed by a node which doesn't have a valid certificate then the packet will be dropped but in other case nodes with valid certificates can conduct the attack, by sending unnecessary route requests or large amount of data packets that can create congestion in the network [9].

3. ATTACKS

MANETs have dynamic topologies, limited physical security and limited resources (power, bandwidth, etc.) due to which they are not secure. Attacks defined in Table -I, all are aimed to adversely affect the availability, confidentiality, integrity and authenticity services. Network attacks are classified under:

- Passive attacks- in these attacks there is no modification of message content, rather they are only aimed to learn contents or other information of communication patterns like- Eavesdropping, etc [7].
- Active attacks- in these attacks message contents are modified to launch different types of attacks like- IP-spoofing, Blackhole, Denial of service attack, etc [7].

3.1 Blackhole Attack

Blackhole attack has been described in [3], [13] and [17] where a malicious intermediate node on receiving the route request packet (RREQ) sends a fake route reply packet (RREP) of having the shortest route. The malicious node doesn't check its routing table and sends an immediate reply by setting hop count to a minimum value (usually 1) and sequence number to a very large value. As the reply from the malicious node is received very fast as compared from the other nodes, the source node will start sending data from the malicious node's path. When such a route is established, it's up to the malicious node which can drop all the received packets or it can forward packets to the unknown address so that packets may not reach the destination node. As discussed in [21] blackhole attack can be of two types:

- **Internal Blackhole attack-** here the malicious node makes itself the part of the routing route by providing fake route replies and does not allow packets to reach to its destination by simply dropping the packets passing through it.
- **External Blackhole attack-** here node stays outside the network and have the control of some internal malicious node of the network.

In ARAN, each node is provided with a certificate so only authenticated nodes can participate in routing; no external node can enter the network. So to compare AODV and ARAN, we are dealing with only internal blackhole attack.

3.1.1 Blackhole in AODV

As discussed in [17], blackhole attack can be conducted by modifying count and sequence number. As shown in Fig-5 a single malicious node has been set, which on receiving the RREQ packet sends a fake RREP packet of minimum hop count and maximum sequence number. Finally the packets which passed through this node would be dropped.

As shown in fig- 5, where node I1 acts as a blackhole node which sends an immediate reply to source node S route request with a RREP packet, where it sets hop_count = 1 and D_seq = 4294967295 [17]. Another genuine RREP packet is sent by node I3 but source node will not accept the RREP packet from node I3 as it has higher hop_count and lower D_seq number as compared to the reply coming from malicious node I1. After this the source node starts sending packets to I1, being the malicious node I1 will drop all the packets without making them to reach the destination node.

3.1.2 Blackhole in ARAN

In ARAN there are no such parameters like hop count or sequence number, for route discovery process. Therefore in

ARAN Blackhole attack is not feasible unless selfish nodes drop the packets [21].

3.2 IP-Spoofing Attack

IP-Spoofing attack has been discussed in [18] where some intruder node sends messages to a node by using the identity of some other legitimate node. The intruder modifies the packet headers such that it appears that the packets are coming from a trusted node.

3.2.1 IP-Spoofing in AODV

AODV is vulnerable to spoofing attack where a node can easily send packets in the network using some other node's identity. These nodes can create congestion in the network by sending large amount of data leading to denial-of-service (DOS) attack. Since the node is using some other node's identity it will be difficult to track the real attacker.

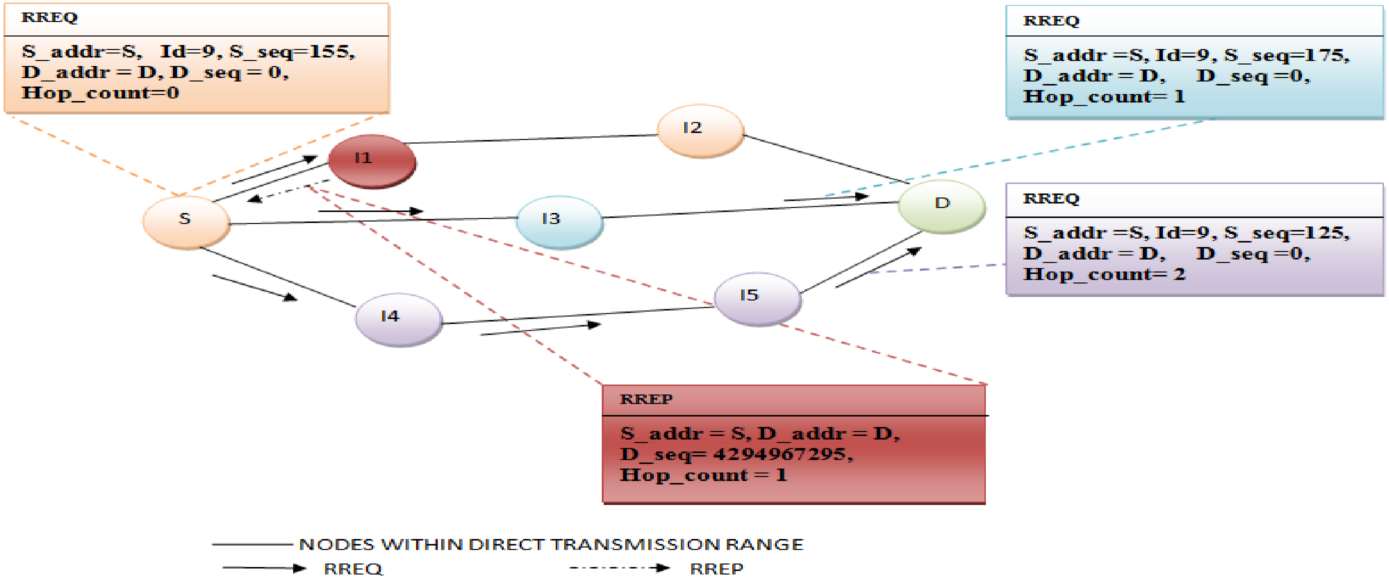
RREQ
S_addr=S, Id=9, S_seq=155, D_addr = D, D_seq = 0, Hop_count=0
RREQ
S_addr =S, Id=9, S_seq=175, D_addr = D, D_seq =0, Hop_count= 1
RREQ
S_addr =S, Id=9, S_seq=125, D_addr = D, D_seq =0, Hop_count= 2
RREP
S_addr = S, D_addr = D, D_seq= 4294967295, Hop_count = 1
S
I1
I2
I3
I4
I5
D
NODES WITHIN DIRECT TRANSMISSION RANGE
RREQ
RREP

Fig -5: Blackhole attack in AODV

3.2.2 IP-Spoofing in ARAN

In ARAN protocol, spoofing is not possible because each node checks the identity of its adjacent node from which it is receiving some information. If any fault is detected in verification process, all the packets are dropped without reaching the destination.

4. SIMULATION APPROACH

The performance evaluation of ARAN and AODV protocols has been done under identical mobility and traffic scenarios in GloMoSim simulator. All simulations are done on an Intel (core i3) machine using Linux Red Hat 9.0 installed on VMWare Workstation 9.

Table –2: Simulation environment setup

Simulation parameter	**Value**
Simulator	GloMoSim-2.03
Simulation Time	100 seconds
Routing Protocols	AODV and ARAN
Traffic	CBR packets
Mobility Model	Random Waypoint
Traffic Sessions	6
Number of nodes	10, 30, 50 and 70
Number of internal Blackhole node	1
Node speed	0 and 15m/s
Terrain Area	500*500, 750*750, 1000*1000 and 1250*1250
Packet size	512 bytes
Performance Metrics	Packet Delivery ratio, Path length, Delay and Throughput

4.1 Traffic

Constant bit rate (CBR) packets are sent over the network.

4.2 Mobility Model

Random Waypoint Model is used to simulate MANETs where the mobile nodes can move randomly in any direction constrained with the speed specified in MOBILITY-WP-MIN-SPEED and MOBILITY-WP-MAX-SPEED parameters of GloMoSim. Also MOBILITY-WP-PAUSE defines the pause time a node pauses before moving randomly further [1], [11].

4.3 Traffic Sessions

To generate traffic 6 nodes are selected as source nodes and 6 nodes as the receiver nodes. All these sending nodes send packets of 512 bytes at the rate of 10 packets per second. Total 100 packets are sent from each node. All the simulations for a particular number of nodes are carried out for two different speeds- 0m/s (no mobility) and 15m/s.

4.4 Terrain Areas for Different Number of Nodes

Simulations are done for different number of nodes which are randomly allocated in different terrain areas. For simulation of 10 numbers of nodes the terrain area is given as 500*500; similarly for 30 nodes it is 750*750; for 50 nodes it is 1000*1000 and for 70 nodes it is given as 1250*1250.

4.5 Performance Metrics

Various metrics are calculated as:

- PDR (Packet Delivery ratio) - This metric indicates the fraction of total data packets reached the destination to the total number of packets sent by the sender and is thus calculated as: Total Packets Received/Total Packets sent [15].
- Average Path length- This is the average length of the paths discovered by the protocol. It is calculated as: Total data packets/Total hops taken [15].
- Average end-to-end Delay (in seconds) - This is the average delay between the sending of the data packets by the source and its receipt at the corresponding receiver [9].
- Throughput (bits/second) - This value represents the ratio of the total bits of data packets that reach their destination, to the total time it takes to reach to the destination.

In the following simulations, performance of AODV protocol under blackhole attack is compared with ARAN protocol.

4.5.1 Experiment 1: Packet Delivery Ratio (PDR)

Fig -6 shows the effect of blackhole attack on packet delivery ratio for AODV and ARAN.

- It has been observed that the packet delivery ratio decreases more under AODV as compared to ARAN. The packet delivery ratio is 16-83% while using AODV but ARAN provides nearly 83-100% PDR in same scenarios.
- The decrease in PDR in AODV is due to the blackhole node which can cause maximum data packets to pass through it by giving fake route reply and finally drops the packets. But in ARAN selfish node cannot send such a reply, so the packets passing through the selfish node can be simply dropped.

It can be said that AODV is highly vulnerable to blackhole attack.

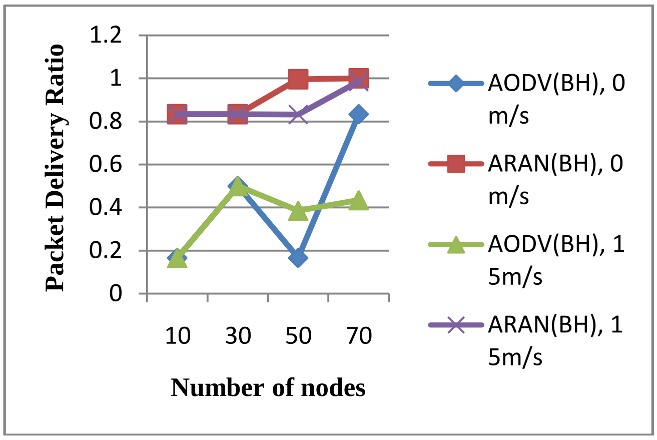

Fig -6: Packet Delivery Ratio of AODV and ARAN under blackhole attack at different speeds and varying number of nodes.

4.5.2 Experiment 2: Path Length

Fig -7 shows the effect of blackhole attack on path length parameter for AODV and ARAN.

- AODV has been observed of having a longer route path in presence of malicious node (from 1 to 3). As the node is moving randomly so depending on its current position to the destination, path length may increase or decrease. In ARAN the packets reach the destination by optimal path (from 1 to 1.1).
- In AODV malicious node can set a longer route path for the packets passing by it. ARAN provides authenticity due to which malicious nodes can't modify contents of the routing packets. Secure routes are selected and there is no adverse effect on the Path length.

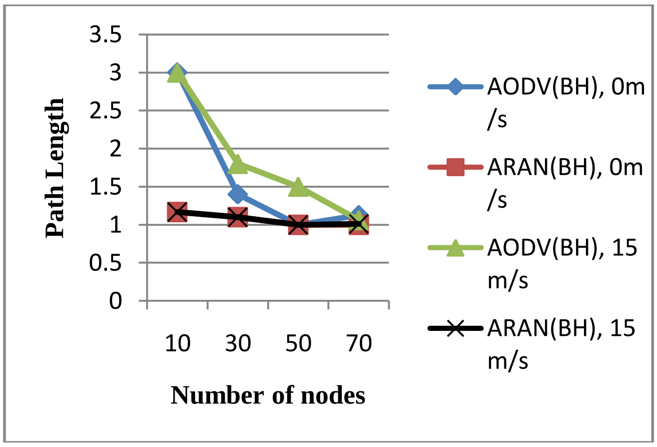

Fig -7: Comparison of Path Length of AODV and ARAN under blackhole attack at different speeds and varying number of nodes.

4.5.3 Experiment 3: Average end-to-end Delay

Fig -8 shows the effect of blackhole attack on delay parameter for AODV and ARAN.

- It has been observed that there is an increase in average end-to-end delay in AODV under the Blackhole attack as compared to that of the ARAN.

In case of 10 nodes where delay of AODV is less although there is an increase of path length as shown above in Fig- 7, this can be due to very less packet delivery ratio of AODV while using 10 nodes (as shown in Fig- 6) due to which average end-to-end delay decreases. Similarly in case of 50 nodes there is high increase in delay of AODV at 15m/s as compared to AODV at no mobility because packet delivery ratio is high.

- Average end-to-end delay depends upon Packet Delivery ratio as well as on Path length. So, it is delay is more in AODV as compared to ARAN.

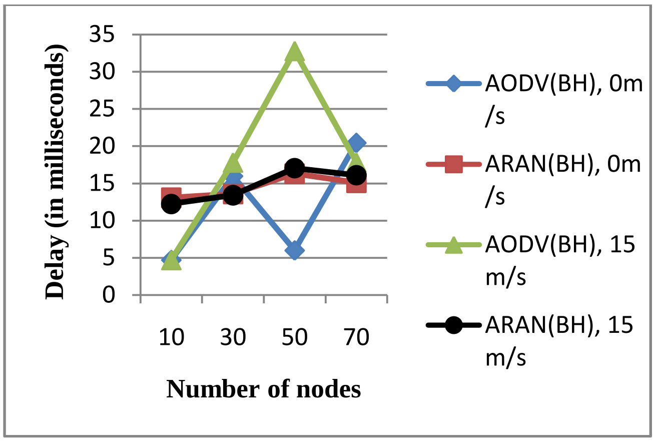

Fig -8: Comparison of Delay of AODV and ARAN under blackhole attack at different speeds and varying number of nodes.

4.5.4 Experiment 4: Throughput

Fig -9 shows the effect of blackhole attack on throughput for AODV and ARAN.

- The throughput of AODV is less as compared to that of ARAN.
- This effect is because of the decrease in Packet Delivery Ratio, as there is a decrease in total number of data bits received so throughput decreases in AODV.

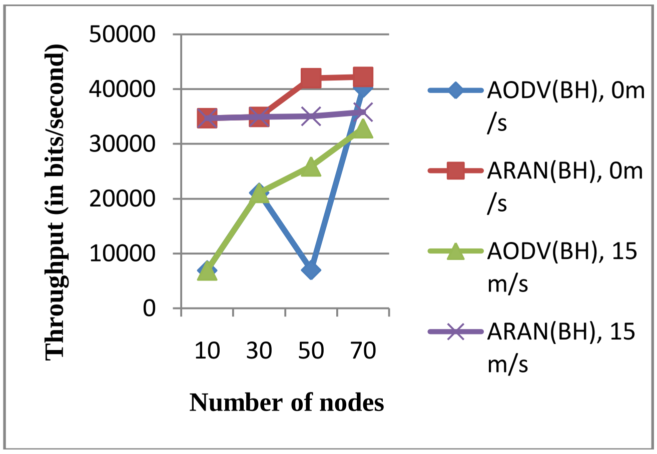

Fig -9: Comparison of Throughput of AODV and ARAN under blackhole attack at different speeds and varying number of nodes.

4.5.5 Experiment 5: Packet Delivery Ratio (PDR) during IP-Spoofing Attack

Results show that nearly 99.9% of spoofed packets reach the destination while using AODV but 0% while using ARAN. Fig -10 shows the effect of IP-spoofing (IPS) attack on packet delivery ratio for AODV and ARAN.

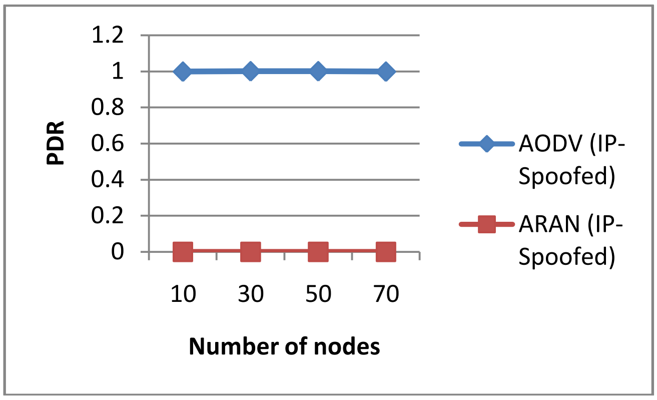

Fig -10: Comparison of Packet delivery ratio of AODV and ARAN in IP-Spoofing Attack.

5. CONCLUSIONS

Apart from the various advantages of adhoc networks over the wired networks, they are vulnerable to variety of attacks, like modification of routing messages, impersonation of other nodes, dropping of packets without making them reach the destination and many more. To overcome this problem many secure routing protocols have been proposed and one of them is ARAN protocol. To analyze its secure functionalities ARAN has been checked against a commonly used reactive routing protocol AODV for Blackhole attack and IP-spoofing. Blackhole attack can be conducted in ARAN protocol only by the selfish nodes which do not forward packets to other nodes. After carrying out various simulations in GloMoSim-2.03 simulator and analyzing various performance metrics it has been observed that ARAN provides higher Packet delivery ratio and Throughput against AODV; also AODV shows more Delay and Path Length than ARAN under blackhole attack. So ARAN provides secure routing as compared to AODV against blackhole attack. Simulation results for IP-Spoofing attacks shows that the spoofed packets reach the destination while using AODV but in ARAN all the spoofed packets are dropped i.e. no packet reached the destination. Thus ARAN is safe against spoofing attack also.

REFERENCES

[1]. L. Bajaj, M. Takai, R. Ahuja, K. Tang, R. Bagrodia, and M. Gerla, "Glomosim: A scalable network simulation environment," *UCLA Computer Science Department Technical Report*, vol. 990027, p. 213, 1999

[2]. D. Benetti, M. Merro, and L. Vigano, "Model checking ad hoc network routing protocols: Aran vs. endaira," in *Software Engineering and Formal Methods (SEFM), 2010 8th IEEE International Conference on*, 2010, pp. 191-202.

[3]. S. Dokurer, *Simulation of Black hole attack in wireless Ad-hoc networks*: Atılım University, 2006.

[4]. L. Ertaul and D. Ibrahim, "Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)," in *Security and Management*, 2009, pp. 363-369.Paper presented at the Security and Management.

[5]. A. Garg and V. Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks," *International Journal*, vol. 2, 2012.

[6]. C. Gong, S. Wu, and Y. Jing, "ARAN protocol analysis and improvement," in *System Science, Engineering Design and Manufacturing Informatization (ICSEM), 2012 3rd International Conference on*, 2012, pp. 347-350.3rd International Conference on.

[7]. S. R. Gowda and P. Hiremath, "Review of Security Approaches in Routing Protocol in Mobile Adhoc Network," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, 2013.

[8]. M. Kumar and K. Gupta, "Secure routing protocols in ad hoc networks: A review," in *Special Issue of IJCCT, 2010 for International Conference (ICCT 2010), December*, pp. 3-5.

[9]. A. Mahmoud, A. Sameh, and S. El-Kassas, "Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)," in *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, 2005, pp. 8 pp.-794.

[10]. S. Mehla, B. Gupta, and P. Nagrath, "Analyzing security of Authenticated Routing Protocol (ARAN)," *International Journal on Computer Science & Engineering*, vol. 2, 2010.

[11]. T. Nilsson, "A Tutorial on GloMosim," *Department of Computing Science. University of Umea*, 2002.

[12]. P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols," *Ad Hoc Networks*, vol. 3, pp. 795-819, 2005.

[13]. J.-C. Ruiz, J. Friginal, D. Andres, and P. Gil, "Black Hole Attack Injection in Ad hoc Networks," in *DSN2008, International Conference on Dependable Systems and Networks. Anchorage, Alaska*, 2008, pp. G34-G35.

[14]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, 2002, pp. 78-87.

[15]. K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, pp. 598-610, 2005.

[16]. H. Shahnawaz, S. Gupta, and C. Mukesh, "Denial of Service attack in AODV & friend features extraction to design detection engine for intrusion detection system in Mobile Adhoc Network," in *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*, 2011, pp. 292-297.

[17]. I. Ullah and S. U. Rehman, "Analysis of Black Hole attack on MANETs Using different MANET routing protocols," *School of Computing Blekinge Institute of Technology, Sweden*, 2010.

[18]. M. Tanase, "IP spoofing: an introduction," *Security Focus*, vol. 11, 2003.

[19]. G. Vigna, S. Gwalani, K. Srinivasan, E. M. Belding-Royer, and R. A. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in *Computer Security Applications Conference, 2004. 20th Annual*, 2004, pp. 16-27.

[20]. Z. Zhou, "Security enhancement over ad-hoc AODV routing protocol," *Tsinghua University, Beijing, zhou-zw02@ mails. tsinghua. edu. cn*, 2007.

[21]. P.Kamra, T. P. Singh, and Dr. R. K. Singh, "Preventing Black hole Attacks in Mobile adhocNetworks: A Review," in *Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering – RTCCE*, 2013.