INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Performance Evolution Of Hybrid-AODV Protocol Using CBR & TCP Connections In MANET

Ms Darshana Patel
M.Tech student,
RCEW, Jaipur,Rajasthan, India

Ms Vandana Verma
Asst.Prof,
RCEW, Jaipur,Rajasthan, India

Abstract:
In this paper authors presents, Some performance measures of hybrid-AODV(Encrypted AODV) for different traffic like CBR & TCP connection for MANET. MANETs are mostly established in insecure environments like disaster sites and military applications. Auhthors measures performance of network using packet delivery fraction & Routing load. AODV is widely used routing protocol in MANETs AODV is the protocol that developed without considering security. After applying security over AODV, performance of AODV degreed sometimes. So after applying encryption process on AODV they measure that packet delivery fraction & routing load increase or decrease using both CBR & TCP connection. Simulation for this experiment they use NS2.34 simulator.

Keywords: *MANETs, CBR, TCP, Performance*

1.Introduction

MANET is a set of independent mobile nodes e.g. cellphoes,Laptops, tablets, pda etc. that communicate over relatively bandwidth and power constrained wireless links. Our strategy is to choosing one of the secure routing protocols among all according to its effectiveness, Authors have study it and analyze its functionality and performance measurements. Then, the different existing security techniques (e.g. encryption algorithm.) were surveyed so that to come up with new algorithm to integrate with the basic AODV protocol. And fortunately, a scheme of integrating encryption algorithm with basic

MS DARSHANA PATEL is M.Tech student of RCEW, Rajasthan, India. Mobile No:9727771064. E-Mail Id : darshana.dhyana@gmail.com

MS VANDANA VERMA is working in RCEW, Rajasthan, India. Mobile No: 9983741634.E-Mail Id :vandana.mtech@gmail.com

AODV routing protocol is found capable of handling both unauthorized and malicious nodes' attacks. Authors are presenting their own work with enhancing the security of AODV routing protocol that protects against a number of attacks carried out in packet routing mechanisms for MANETs. Authors would present their encryption algorithm to secure AODV messages which they have implemented on existing AODV protocol in NS-ALLINONE. Here they measure packet delivery fraction and Routing Load using CBR & TCP connection.

2.AODV Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) is inherently a distance vector routing protocol that has been optimized for ad-hoc wireless networks. It is an on demand protocol as it finds the routes only when required and is hence also reactive in nature. AODV borrows basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. To avoid the problem of routing loops, AODV makes extensive use of sequence numbers in control packets.

When a source node intends communicating with a destination node whose route is not known, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains an ID, source and the destination node IP addresses and sequence numbers together with a hop count and control flags. The ID field uniquely identifies the RREQ packet; the sequence numbers inform regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Each recipient of

the RREQ packet that has not seen the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain interval of time.

When the RREQ packet reaches the destination node or any node that has a fresher route to the destination a RREP (Route Reply) packet is generated and unicasted back to the source of the RREQ packet. Each RREP packet contains the destination sequence number, the source and the destination IP addresses, route lifetime together with a hop count and control flags. Each intermediate node that receives the RREP packet, increments the hop count, establishes a FORWARD ROUTE to the source of the packet and transmits the packet on the REVERSE ROUTE.

For preserving connectivity information, AODV makes use of periodic HELLO messages to detect link breakages to nodes that it considers as its immediate neighbors. In case a link break is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route.

Optionally,aRoute Reply Acknowledgement (RREP-ACK) message may be sent by the originator of the RREQ to acknowledge the receipt of the RREP. RREP-ACK message has no mutable information. The Message Formats of AODV routing protocol is shown in Appendix F.

There are two phases of AODV routing protocol: Route Discovery Phase and Route Reply Phase.

2.1.Route Discovery

2.1.1. Route Request Stage

The source node floods the network with a route request control packet (RREQ), and each node (with the exception of destination) rebroadcasts the RREQ the first time it hears.

2.1.2.Route Reply Stage

upon receiving a RREQ, the destination sends a route reply packet (RREP), which is propagated to the source in the reverse path of the RREQ.

2.2.Route Maintenance

If an intermediate node is unable to transmit a data packet to the next hop in the path, it sends a route error control packet (RERR) to the source to inform the broken route.

3.Hybrid-AODV Protocol.

Hybrid-AODV(Encrypted-AODV) Algorithm as follows:

- In routing of AODV, sender node generates the signature using an encryption algorithm and concate it with each of the AODV messages. It performs the following operations:

- It uses secure hash algorithm (SHA) value to generate signature.
- Sets signature SHA value with the message format.
- Now for specially destination node sender uses public key to generate another signature and generate the same and also concate it with message.

- Afterwards, each time an intermediate node receives sent message, it calculates the following calculations to verify the genuine message:

- It uses the concated signature to match the newly generated signature by intermediate node and compare it; if it matches then node will forward the message to the next node.
- But before rebroadcasting a message it will check the index of upcoming node to check whether it is destination or not.

- Finally, if receiving node matches the value of index and find it is destination node then, it will calculate the signature with using public key for more security purpose and compare it with concated special signature with key.

4.Connection Types

Several kinds of connection patterns are available. In our simulation we use CBR & TCP connection.

4.1.Constant Bit Rate(CBR)

CBR is also consistent bir rate means packets sent with fixed size and fixed interval between each packets. In which connection between node is not required. Receiving node don't send any acknowledgement. Connection establish only one way from source to destination.

4.2.Tranmission Control Protocol(TCP)

TCP is connection oriented. It use acknowledgement, time-outs and retransmission for reliability from source to destination.

5.Performance Matrics And Network Parameters

5.1.Packet Delivery Fraction(PDF)

PDF=Noof received packets /No of sent packets

5.2.Routing Load(RL)

RL= No of routed packets /No of received packets

5.3.Network Parameters

Parameter	Value
MANET Area	500*500 sq. m.
Total number of	25
Movement Pattern	Non-random
Node Speed	0 up to 20 m/s
Application	Constant Bit Rate (CBR), Transfer Control
No. of generated Packets	10000 packets per CBR
Size of Packet	512 bytes
Simulation Time	100 sec
CBR Traffic / TCP traffic	5-10-15-20
Pause Time	0-10-20-40-100

Table 5.1: General Simulation Parameters

6. Our Simulation

6.1.Experiment 1

Packet Delivery Fraction

PDF=Noof received packets /No of sent packets

The packet delivery ratio is directly influenced by packet loss, which may be caused by general network faults or uncooperative behavior.

In this experiment PDF measured for H-AODV using CBR & TCP connection

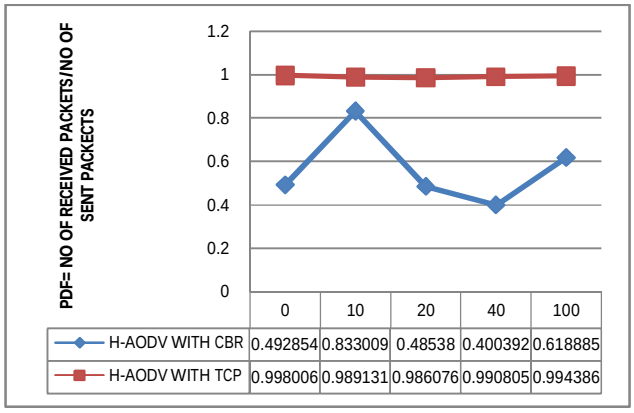

Figure 6.1:PDF for 5 CBR/TCP connection

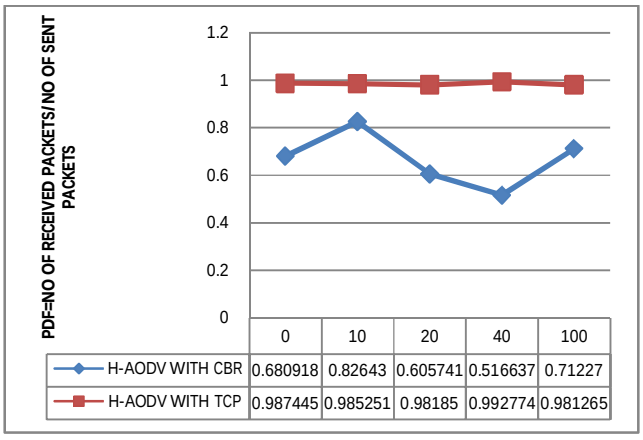

Figure 6.2:PDF for 10 CBR/TCP traffic

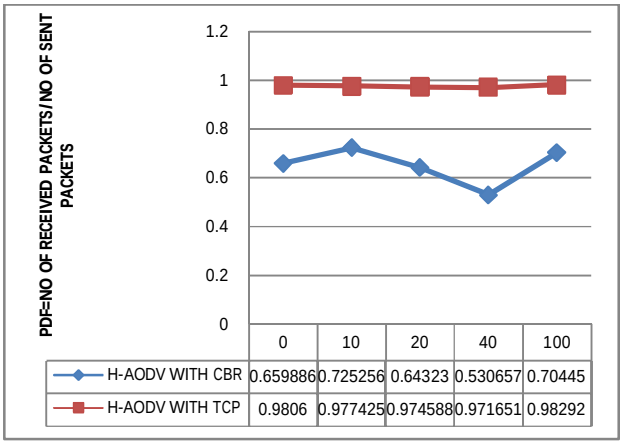

Figure 6.3: PDF for 15 CBR/PDF traffic

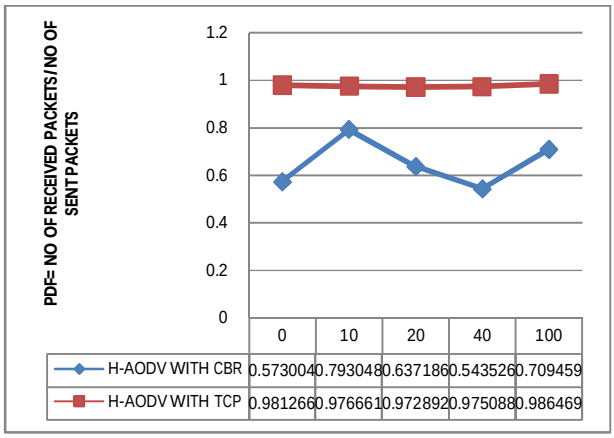

Figure 6.4: PDF for 20 CBR/PDF traffic

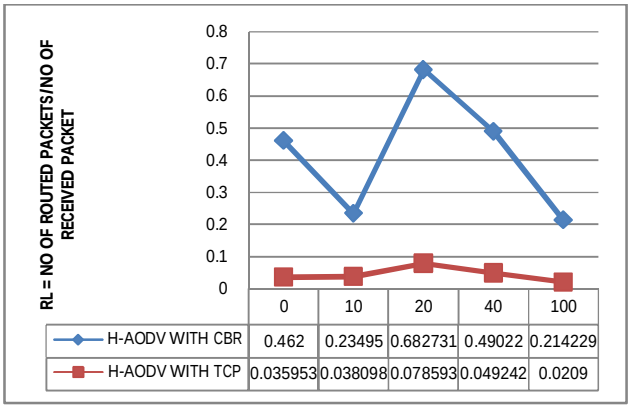

Figure 6.5: RL for 5 CBR/TCP traffic

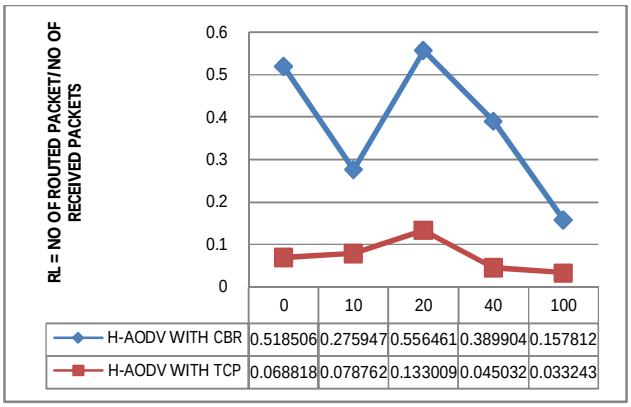

Figure 6.6 : RL for 10 CBR/TCP traffic

6.2.Experiment 2: Routing Load(RL)

RL = No of routed packets/ No of received packets

In this Experiments we measure RL for H-AODV for CBR & TCP Connections

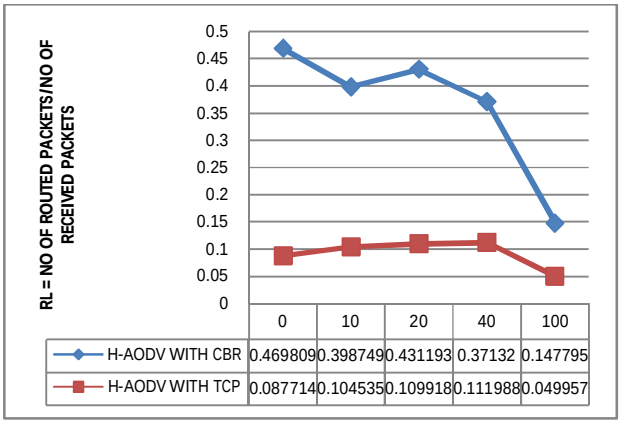

Figure 6.7: RL for 15 CBR/TCP traffic

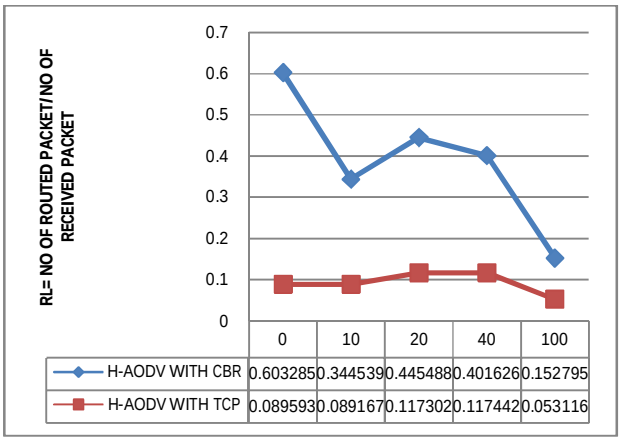

Figure 6.8: for 20 CBR/TCP traffic

7. Conclusion

This paper analyze performance evolution of Hybrid AODV protocol using CBR and TCP Connection.

From our experimental analysis, we analyze that for Hybrid AODV protocol the packet delivery ratio is higher using TCP Connection than CBR Connection. While Routing Load is lower using TCP connection than CBR Connection.

So we conclude that our Hybrid AODV give better performance using TCP connection rather than CBR Connection.

8.Reference

1. Pirzada, McDonald, "Secure Routing with the AODV Protocol" (2005) IEEE pp.57-61
2. Stephan Eichler and Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", Aug 2006.
3. Chee-Wah Tan, Sanjay Kumar Bose, "Modifying AODV for Efficient Power Aware Routing in MANETS", (IEEE) 2005
4. Lu Jin, Zhongwei Zhang, Hong Zhou, "Performance Comparison of the AODV, SAODV and FLSL Routing Protocols in Mobile Adhoc Networks", Year: 2007
5. Sandhya Khurana Neelima Gupta and Nagender Aneja, "Reliable Ad-hoc On-Demand Distance Vector Routing Protocol", (IEEE) Year: 2006, 0-7695-2552-0/06
6. Alaa S. Dalghan, Mohamad M. Gamloush, Raji M. Zeitouny, and Yasser M. Shaer, "Securing Mobile Adhoc Networks"
7. Yih-Chun Hu, "A Survey of Secure Wireless Adhoc Routing", (IEEE) 2004
8. Tuulia Kullberg, "Performance of the Ad-hoc On-Demand Distance Vector Routing Protocol", 2004
9. Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, "Experimental Comparisons between SAODV and AODV Routing Protocols", ACM 2005
10. Kimaya Sanzgiri, Bridget Dahill, "A Secure Routing Protocol for Ad Hoc Networks", IEEE, 2002
11. Durgesh Wadbude, Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET", IJEIT, 2012
12. Monis Akhlaq, Nomal Jafri et al. "Data Security Key Estalishment in AODV", WSEAS, 2007
13. Junaid Arshad, Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", (2006) IEEE, pp. 971-975.
14. Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE 2008
15. The Network Simulator – NS2. (http://www.isi.edu/nsnam/ns/index.html)
16. The ns Manual, (formerly ns Notes and Documentation) The VINT Project a Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, Kevin Fall, pp. 160