International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

IJERMT Email: editor@ijermt.org March- 2014 Volume-1, Issue-2 Website: ijermt.org

A SECURED: WIRELESS PROTOCOL USING RSA

NITIN JIRWAN, SHWETA BHATNAGAR, Dr. SANDIP VIJAY
Department of Electronics & Communication Engineering
D.I.T. Dehradun

Abstract-
In this paper comparative work on data packet and byte delivering, throughput and average end-to-end delay in simple AODV and AODV with RSA encryption algorithm is done. In simple AODV, when blackhole attack is applied then there is a serious degradation in results mentioned earlier which decreases the efficiency of AODV routing protocol. So to increase the efficiency of AODV, RSA encryption algorithm is applied and simulated in QUALNET simulator, which gives better results than simple AODV protocol.

Key words-- RSA, attack in AODV, AODV security.

I. INTRODUCTION

In Qualnet simulator, have only AODV protocol [1]. For comparison of work, attacked and encrypted AODV is needed. So attack program is written in C++ and added on simple AODV. After adding we applied this attack AODV on multiple nodes. Then it gives decreasing results. Now RSA algorithm[3] is written in c++ and added on that attack AODV protocol. Same we applied this encrypted attack AODV on same previous nodes, and then it gives increasing results. Asymmetric key technique is analyzed over an attack by using ad-hoc protocol. Some asymmetric techniques are RSA(Rivest Shamir and Adleman)[2], protocol.

II. RSA

RSA(Rivest Shamir and Adleman)(furozan): In this method, one party (a bank customer ,for example) uses a public key, Kp. The other party uses the secret (Private) key, Ks. Both use a number, N.

➢ The encryption algorithm follows these steps [3]:

- Encode the data to be encrypted as a number tocreate the plaintext P.
- Calculate the cipher text C as C=PKp modulo N (modulo means divide PKp by N and keeps only the remainder).
- Send C the cipher text.

➢ The decryption algorithm follows these steps:

- Receive C, the cipher text.
- Calculate plaintext P= CKs modulo N.
- Decode P to the original data.

III. ATTACK

Attack in AODV: Firstly false node attack is developed in to a network. It is false node attack we can say its black hole attack. It injected to false information into the network. The network information (packet) is destroyed by this attack [4].

IV. SECURITY

AODV security: Now RSA encryption & decryption algorithms are added in AODV. We know that RSA have public key and private key. It means that source node have private key for encryption and all nodes have public key for decryption except false node. When false node is trying to receive the information, then previous node will match key if false node don't have key then request of false node will be denied. So that our network can be saved by RSA encryption [5].

This process is done in Qualnet Simulator [6]. Before simulating these scenarios we have to add black hole attack and RSA encryption in network layer.

V. RESULT

A. Discussion of Results:

In this section three scenarios **1**. Simple AODV **2.** Black Hole attack on AODV **3**.RSA security technique on AODV routing protocol are studied. In first scenario packets are sent using simple AODV protocol, in second scenario packets are sent using attack AODV and in third case RSA cryptography algorithm is used with AODV for sending data packets for source to destination with same attack. Packets are sent over different no. of nodes and analyzed in following sub sections

B. Simulation Results and Analysis:

50 nd 100 nodes are taken in Qualnet simulator

a. Packet delivered and received: In the first scenario we have to check how many packets are received by RSA. So we check three sub scenarios. These are given below.

1. **Packet delivered:** In this scenario, figure1 shows all 24 packets are successfully delivered.

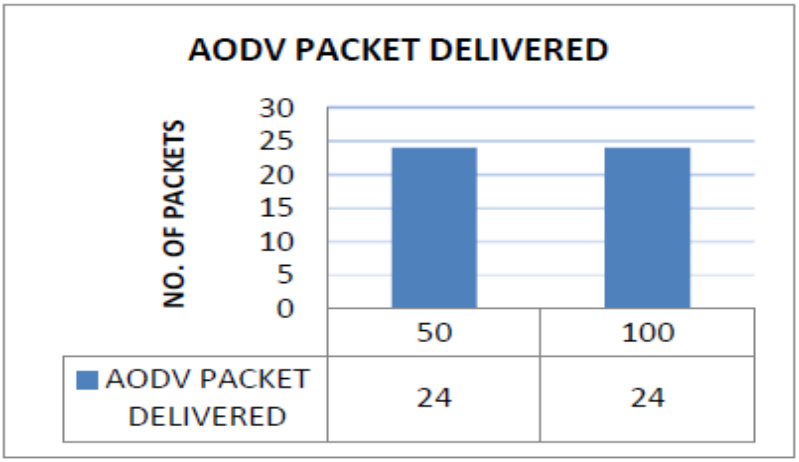

Fig.1 Packet delivered

2. **Packet received after attack:** In this scenario we check how many packets received after attack. Figure2 shows that, in 50 nodes zero packet is received and in 100 nodes 6 packet are received.

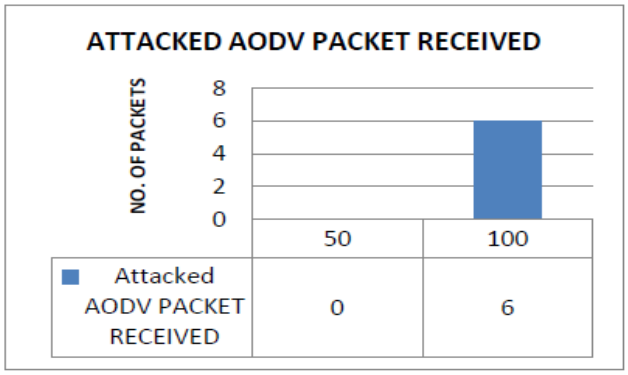

Fig.2 Packet received (attack)

3. Packet received after RSA: In this scenario we apply RSA on attacked AODV. Then figure3 shows in 50 nodes 10 packets are received and in 100 nodes 18 packets are received.

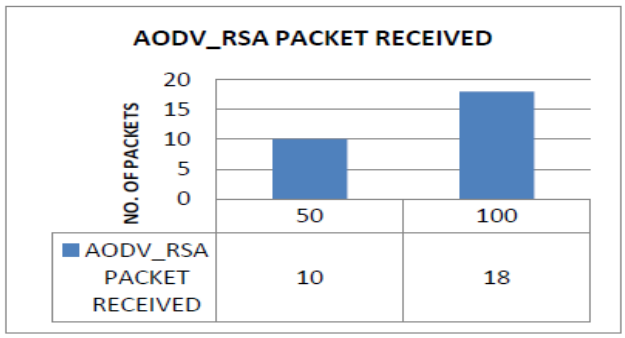

Fig.3 Packet received(RSA)

b. Byte sent and received: In this scenario we have to check how many bytes are received by RSA. So we take 3 sub scenarios.
These are given below.

1. **Total bytes sent:** In this scenario, figure 4 shows 12000 bytes are successfully sent.

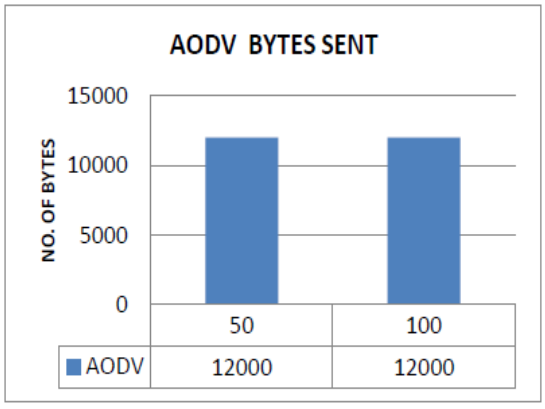

Fig.4 Bytes sent

2. **Total bytes received:** In this scenario, we apply attack on AODV then figure5 shows that in 50 nodes 0 byte is received and in 100 nodes 3200 bytes are received.

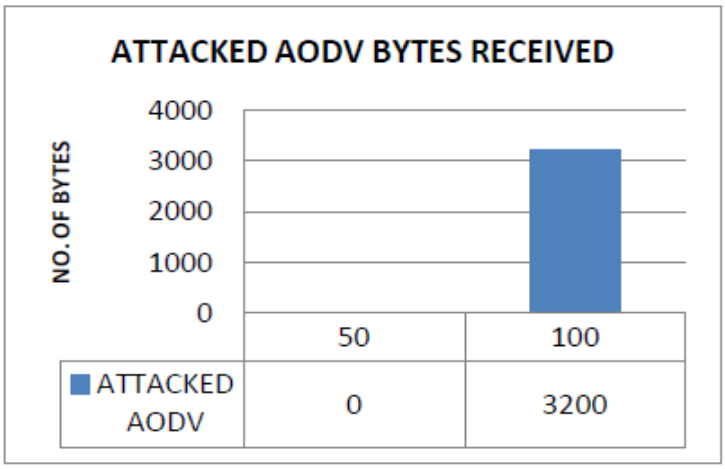

Fig.5 Bytes received(attack)

3. Total bytes received after RSA: Now we apply RSA on AODV, then figue 6 shows that in 50 nodes 4500 bytes are received and in 100 nodes 9000 bytes are received.

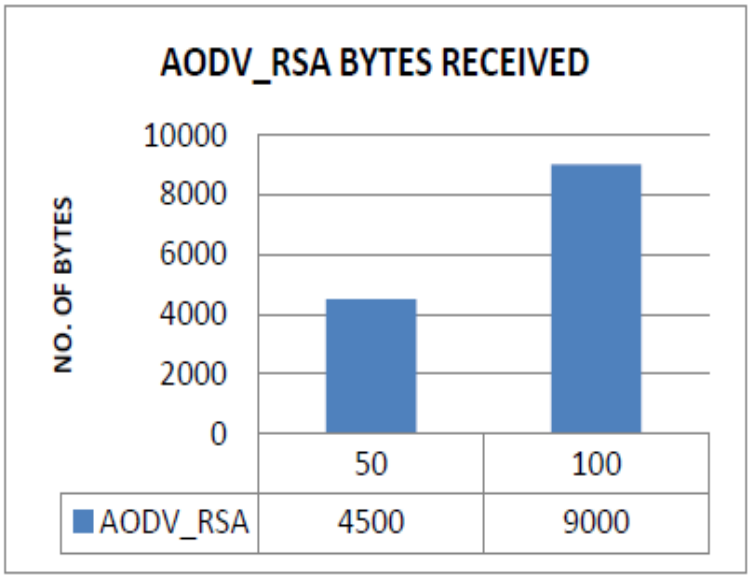

Fig.6 Bytes received(RSA)

c. Troughput: In this scenario we have to check throughput after RSA. Throught means no. of bits transfer in a second. We take three sub scenarios

1. AODV throughput: in this scenario, figure7 shows that 4000bps is throughput in 50 nodes and 100 nodes.

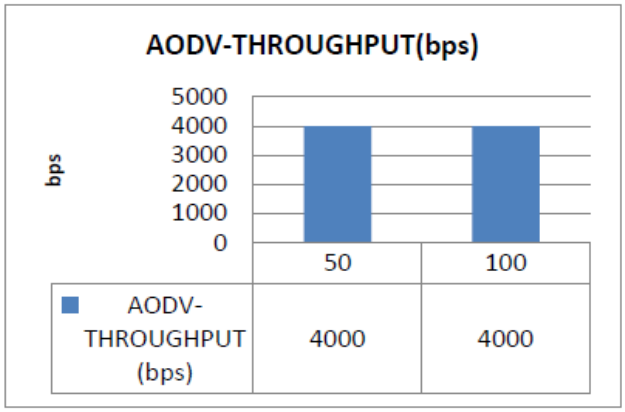

Fig.7 Throughtput

2. **AODV throughput after attack:** When we apply attack on AODV then figure8 shows that in 50 nodes throughput is 0bps and in 100 nodes throughput is 1100bps.

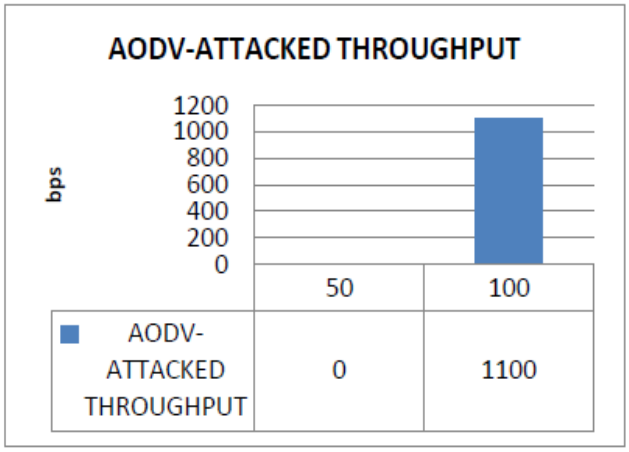

Fig.8 Throughput (attack)

3. Throughput after RSA: When we apply RSA on AODV then figure 9 shows that in 50 nodes throughput are 1600bps and in 100 nodes throughput is 3200bps.

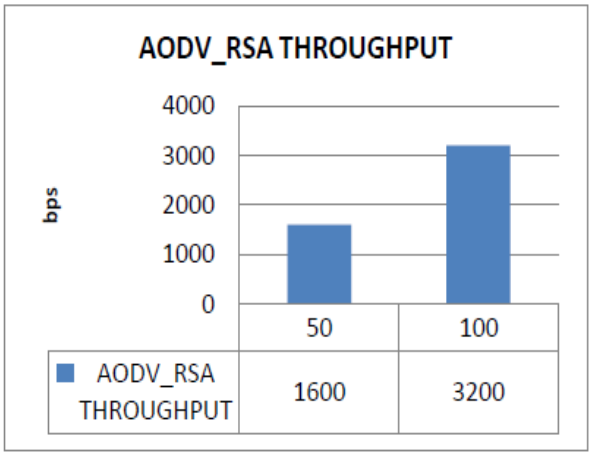

Fig.9 Throughput(RSA)

D. Delay: In this scenario we have to check delay. Delay is checked in destination node. We take two sub scenarios:

1. **Average end to end delay**: In this scenario when we apply attack on AODV then figure 10 shows that in 50 nodes 0 second delay and in 100 nodes 1.2 second delay

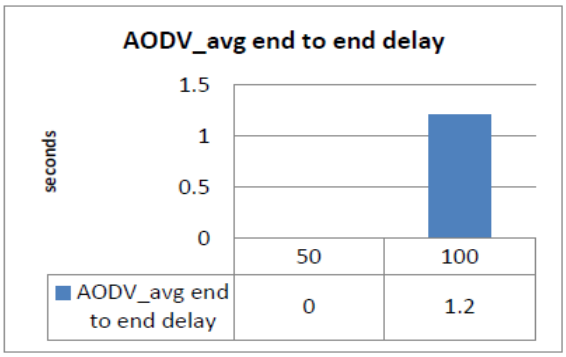

Fig.10 Avg end to end delay

.

2. **Average end to end delay after RSA:** When we apply RSA on AODV then figure 11 shows that in 50 nodes delay is 0.12 second and in 100 nodes delay is 0.1 second.

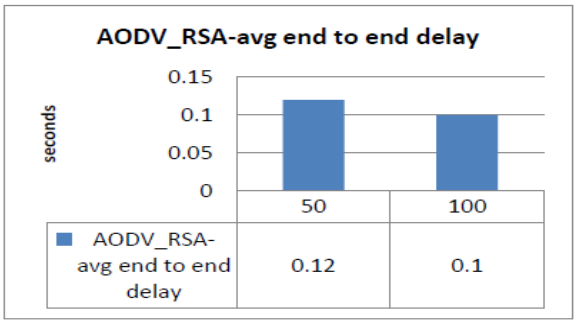

Fig.11Avg end to end delay(RSA)

VI. Conclusion:

Now 4 scenarios are calculated. RSA can surely work in AODV and Ad- hoc network. In all 4 scenarios RSA is doing better work on attacked AODV. RSA have a small mathematical method of prime nos. So whole mechanism is fastly encoded and decoded for any information. Today application we use RSA in less data security not for high data.

Refrences

1. Siva Ram Murthy and B. S. Manoj, "Ad-Hoc Wireless networks," ISBN, 0132465698, 9780132465694 pearson publication, 2012.
2. Wikipedia, http://en.wikipedia.org/wiki/RSA_(algorithm), Dated: 12-dec-2013 at 19:40.
3. A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No.653.2004.
4. M. Arora, Rama Krishna Challa, "Performance Evaluation of Routing Protocols Based on Wormhole Attack inWireless Mesh Networks," 978-0-7695-4042-9/10 © 2010 IEEE DOI 10.1109/ICCNT.2010.34
5. Li Zhe, Liu Jun, Lin Dan, Liu YeA, " Security Enhanced AODV Routing Protocol," Lecture Notes in Computer Science, Volume 3794, 2005, pp 298-307.
6. Web, http://web.scalable-networks.com/content/qualnet, Dated: 12- dec-2013 at 21:05.