Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Experimental Study and Analysis of security on AODV

Khanderia Arzoo[1], Trishla Shah[2]

[1]Department of Computer Engineering, B.H. Gardi College of Engineering and Technology
[2] Prof. At Department of Computer Engineering, B.H. Gardi College of Engineering and Technology

Abstract* — MANET is one of the most promising areas in research. MANET is infrastructure less network with various characteristics like open medium, dynamic topology, scalability etc. But due to these characteristics it is suffering from security aspects. Thus security can be more important in today's world. MANET is used for communication among moving nodes and when security of message is concern it must provide services like confidentiality, integrity, Authentication etc. Various security protocols are designed to avoid various attacks but still show performance issues like high overhead, high delay, less throughput, packet delivery ratio is high etc. Thus it can be said that when we add security its performance decreases. Our paper shows experimental study of AODV and security on AODV. We have compared the results of AODV and secure AODV (based on RSA).

***Keywords-* AODV, Security, RSA, Security Attack, Performance analysis.**

I. INTRODUCTION

MANET is self-configured network. In this network, each node work as Adhoc without any infrastructure and is mobile so its topology changes frequently. Other network than MANET, communication between each node takes place using access point while in case of MANET communication takes place directly without infrastructure. In MANET each node act as router as well to transfer the packets or message between sources to destination. As in MANET changing topology and routing is complicated it is good research work to make simple and efficient. When changing topology is taken into account it becomes necessary to have efficient and secure routing in network. MANET can be explained from following figure.

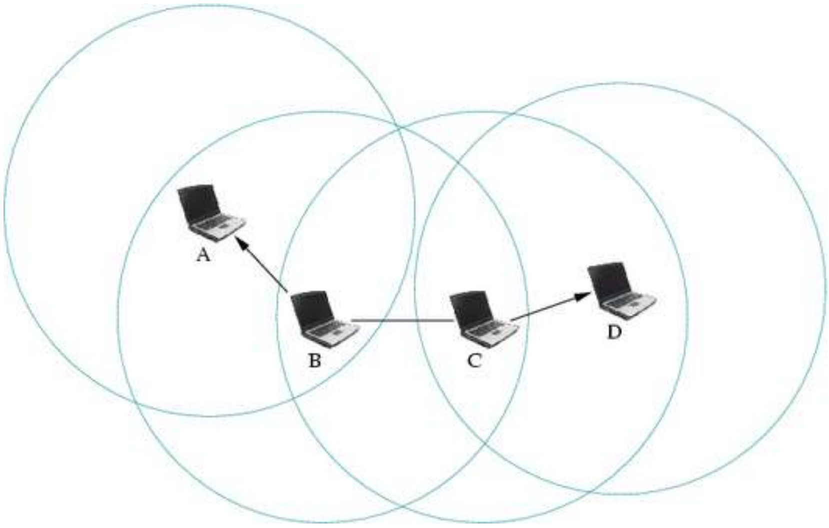

Figure 1. Ad Hoc Network [11]

MANET characteristics are as follows[3]:

1) Dynamic topology
2) Limited energy
3) Self-operated
4) Infrastructure less
5) Bandwidth constrain

A. Routing in MANET

Routing protocols are mainly used to have route from source to destination to overcome overhead issue. There are mainly three types of routing protocols which includes:

- Proactive: Each nodes maintains one or more nodes to store routing information.
- Reactive: It is on demand. The source checks route cache and if does not have route. It initiate route discovery.
- Hybrid: Combination of both in order to overcome the issue of both the protocols.

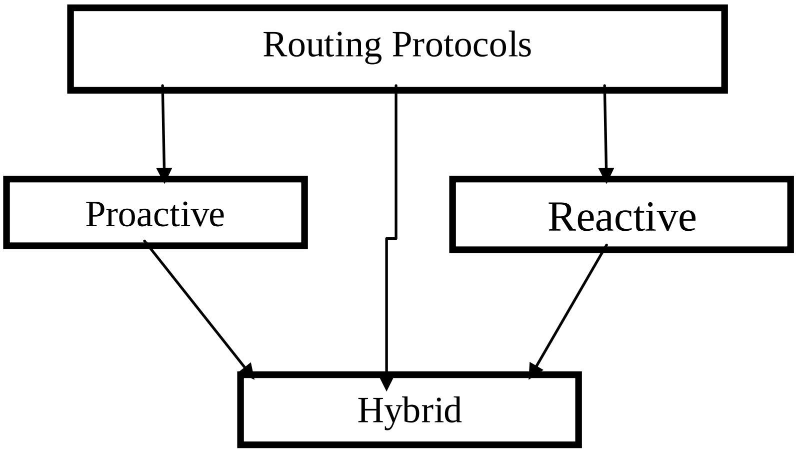

Figure 2. Routing protocol

All the three protocols have their own advantages and disadvantages as per their designed. For example proactive and reactive protocols are designed such that it is easy to understand but create high overhead. Let's we have brief about various routing protocol and its disadvantages and advantages in brief. Below table gives survey on it.

Parameter	Proactive	Reactive	Hybrid
Routing scheme	Table driven	On demand	Combination of both
Routing overhead	High	Low	Medium
Loop Free	Yes	Yes	Yes
Complexity	Less	Less	High
Future challenges	Security and QOS etc.	Security and fault tolerance etc.	Security, QOS etc.

Table 1: Survey of Protocols

A. Security Aspects

For better security in routing one must be aware about the security requirements. As security is broad and essential in computer networks need to have brief about different kinds of attacks and security requirement in network. There are various kinds of security attacks like fabrication, modification, cyclic attack etc. Basically there are two types of attacks [2].

1) Active attacks: These attacks basically destroy the communicating information and degrade the network performance. Attacker can modify and fabricate the information in communicating packets easily.

2) Passive attacks: The attacker is capable to identify the network communication and disturb the network communication. This attack can easily hijack the network information or delay the network communication. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Security goals and requirements [3]:

- ✓ Availability:
- ✓ Confidentially
- ✓ Authentication:
- ✓ Integrity
- ✓ Non repudiation

II. AODV PROTOCOL

AODV is Ad hoc on demand distance vector. AODV is basically an improvement of DSDV. But, AODV is a reactive routing protocol instead of proactive. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination.
AODV performs in two ways:

1) Route discovery: When nodes have data packets to send it starts route discovery process for finding destination route. It sends RREQ packet to neighbors and finds the route. Destination in turn sends RREP reply to source using less hop count method. Then source starts to send data packets to destination.

2) Route maintenance: Route maintenance is done with two control message Hello and RRER. Hello message is used to prove the connectivity [1]. When it does not receive the hello message then it detects the link failure and generate RRER message. This RRER message is forwarded to neighbors and that will erase the route to destination from their table. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message must be sent by sender node of RREQ in response to a RREP message. This provides assurance to the sender of RREP that the link is bidirectional. Each node maintains a routing table with knowledge about the network. AODV deals with route table management.

III. RSA METHODOLOGY

RSA is one of widely used algorithm all over the world. And has many applications. But still it suffers from security aspects. Many researchers have proved that RSA suffers from many cyber-attacks. RSA consist of three phases [5]:

1) Key generation.

- ✓ Select p and q both prime number, p is not equal to q.
- ✓ Calculate n = p x q.
- ✓ Calculate ø (n) = (p -1) x (q-1).
- ✓ Select integer e whose gcd (Ø (n), e) = 1; 1 < e <Ø (n).
- ✓ Calculate private key d = e-1 (mod Ø (n)).
- ✓ Public key PU = {e, n}(sending to receiver)

- ✓ Private Key PR = {d, n}(decrypted by receiver)

2) Encryption

- ✓ Plaintext- Message (M)
- ✓ Cipher text- C = M^ e mod n.

3) Decryption

- ✓ Cipher text- C
- ✓ Plaintext- M = C^ d mod n.

VI. LITERATURE SURVEY

Charles E. Perkins et al [1], have described briefly about basic working of AODV protocol. AODV protocol uses the sequence number concept which is used to indicate fresh route concept as well as loop free path. AODV is on demand protocol so it it establish path whenever it is require to do. AODV protocol is divided into two sections: Route discovery and Route maintenance. AODV uses three messages to communicate RREQs, RREPs, and RRER which is used for request, reply and error message. Here security enhancement is not done so future feature can be security quality services.

Chirag Tehlanl et al [2], have describe about survey different threats on MANET. It also describes the different attacks on different layer and its solution. Here each attack is described briefly like external, internal, DOS attack, Jamming, SYN Flooding, Black hole attack, wormhole attack as well as its comparison to know drawback of each.

Muhammad Saleem Khan et al [3], described bout brief about analysis of Reactive and proactive protocols under security attacks. And also showed performance analysis such as end to end delay, packet delivery ratio, and normalized routing load. Such analysis is carried out in order to find that such protocols are designed without security aspects and as a result performance decreases. So technique must be invented to avoid various attacks.

Ashish Shrma et al [4] have proposed new algorithm which attacks RSA Scheme. Thi scheme obtain the factoring the modulus based on small private key d of RSA scheme. This method is effient under certain circumstances but slow when had larger number of iteration. So future scope can be enhancement in computing speed.

Ritu Partidar [5] gives concept of speeding up the implementation of RSA algorithm during data exchange across the network.A database system is used in order to store key parameters of RSA cryptosystem before it starts the algorithm. Though provides better performance than RSA but still security and efficiency can be concern

Qing Liu [6], as RSA have more computation time this paper uses two varients of RSA in order solve the speed problem. BMRSA (Batch Multi-Prime RSA) speeds up RSA decryption by combining the Multi-Prime RSA and Batch RSA. EAMRSA - Encrypt Assistant Multi-Prime RSA) The experimental results show that the speed of the two variants decryption has been substantially improved. But still for better performance and security its parameter must be optimized.

Sisily Sibichen[7] have proposed a new protocol in order to remove malicious nodes and for that they have done spanning tree fashion and enhanced security by using RSA key exchange protocol. An RSA key exchange and two encryption techniques are used among authenticated neighbor's in the adhoc network to provide more security and thus avoid group rekeying problems.But still creation of spanning tree and detecting fake nodes takes time and along with RSA seems to be less secure and had still suffers from attacks.

Prachi D. Gawade [8] The failure of the link will degrade its characteristics as when the error message is sent back to source and the process get repeated. so proposing a method when nodes or links fails to receive the data packets. Cryptography technique RC6 is used secure the network.In this delay ,PDR is high

Sunil J. Soni[9] proposed a novel security mechanism that integrates digital signature and hash chain to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes with marginal performance difference. The proposed security mechanism was also simulated in the Network Simulator 2 (NS2) to show marginal performance difference under attack**.** Delays are high.

Ali M. Sagheer[10] have used Identity Based Cryptography (IBC) that have many advantage compared to traditional cryptosystems for Secure AODV routing protocol.this can help network to prevent itself from unauthorized nodes,and gives less timings.this method though is more efficient but still suffers from performance issue.

VII. SIMULATION RESULT ANALYSIS

The simulation results are presented. Here we have compared AODV and RSA on AODV. Here is the simulator parameter used in simulation.

Tool	NS-2.35
Simulation Time	100 sec
Topology	Random
Routing protocol	AODV
Number of Nodes	Varies accordingly to measure results
Traffic type	512 byte CBR

Table 2: Simulation parameter

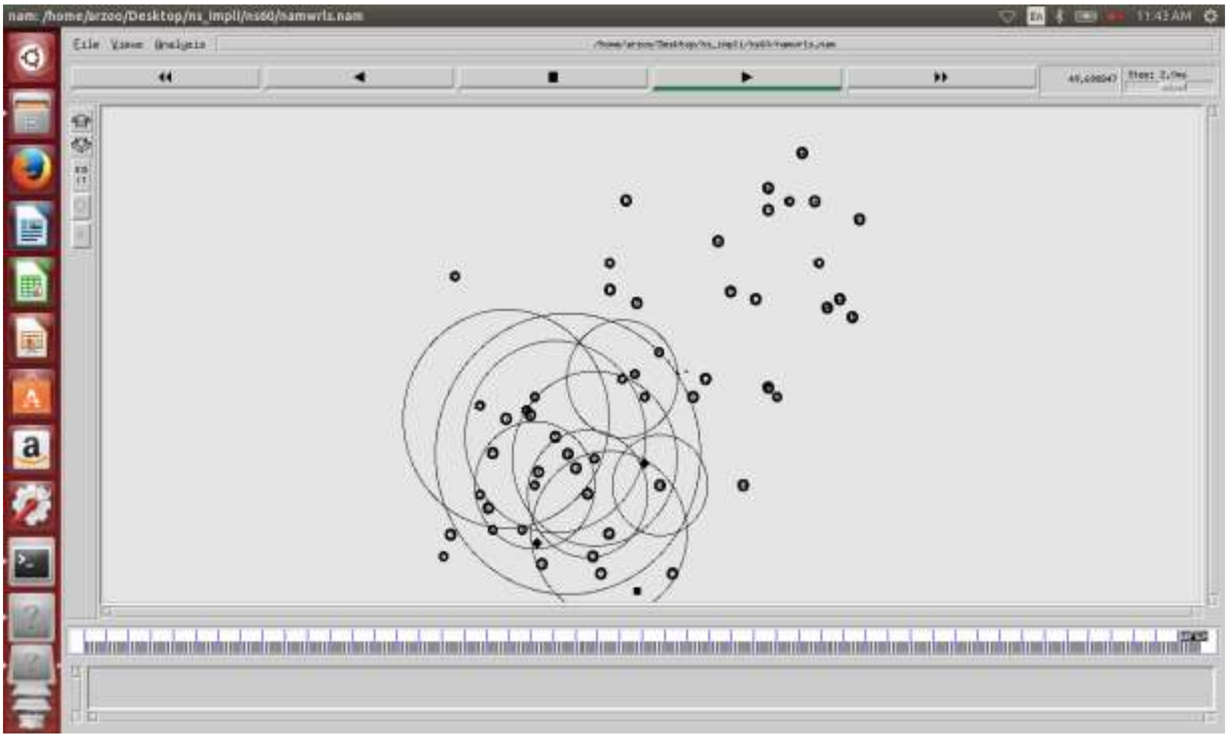
nam: /home/arzoo/Desktop/ns_impli/ns60/namwrls.nam
11:43 AM
File
Views
Analysis
/home/arzoo/Desktop/ns_impli/ns60/namwrls.nam

Figure 3. Simulation of mobile nodes in AODV

As we have implemented, it can be concluded that as number of nodes increases their throughput and good put increases while packet delivery ratio decrease. Let we compare the performance aspects of normal AODV and secure RSA on AODV.

- **Throughput**
  - Rate of Successful message delivery over a communication channel.

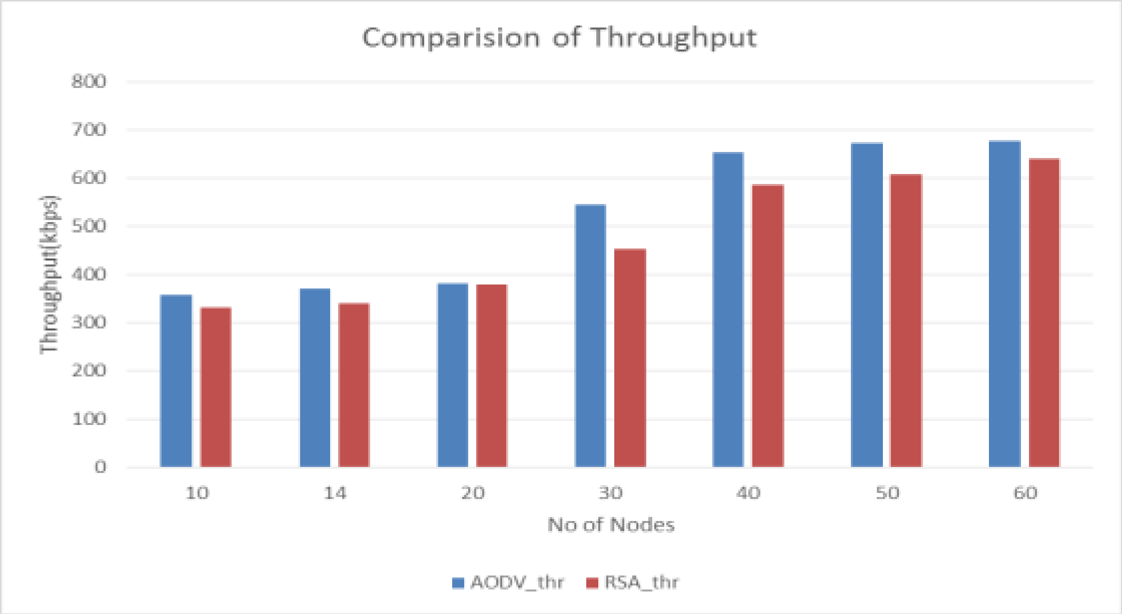

Figure 4: Camparision throughput graph of AODV and RSA on AODV

- **PDR(Packet delivery ratio)**
  - Ratio of number of delivered data packets to destination

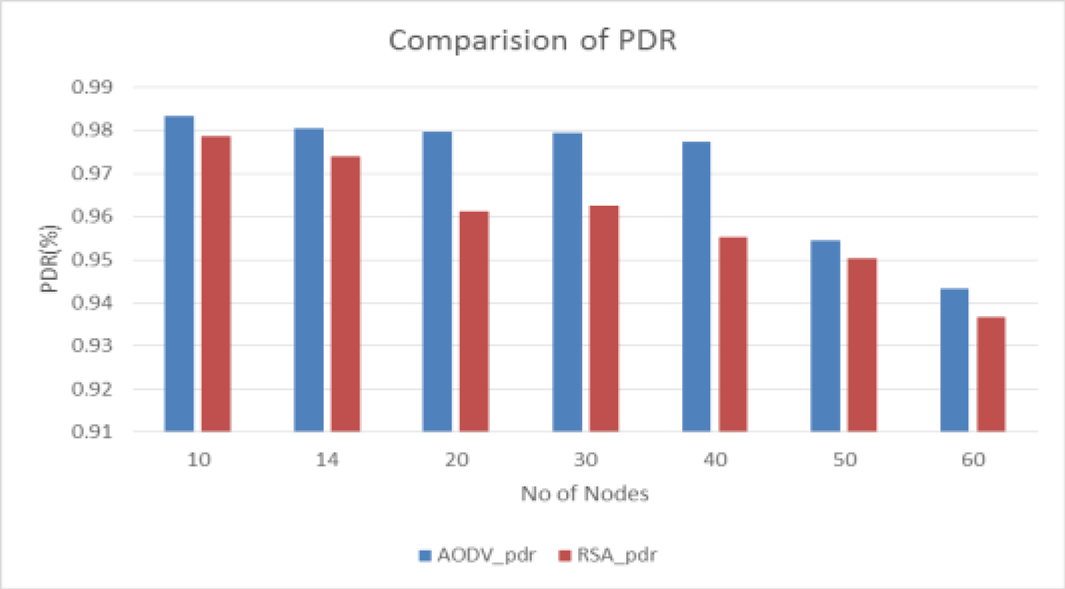

Figure 5: Camparision PDR graph of AODV and RSA on AODV

- **Good put**
  - Rate at which useful data travels a link

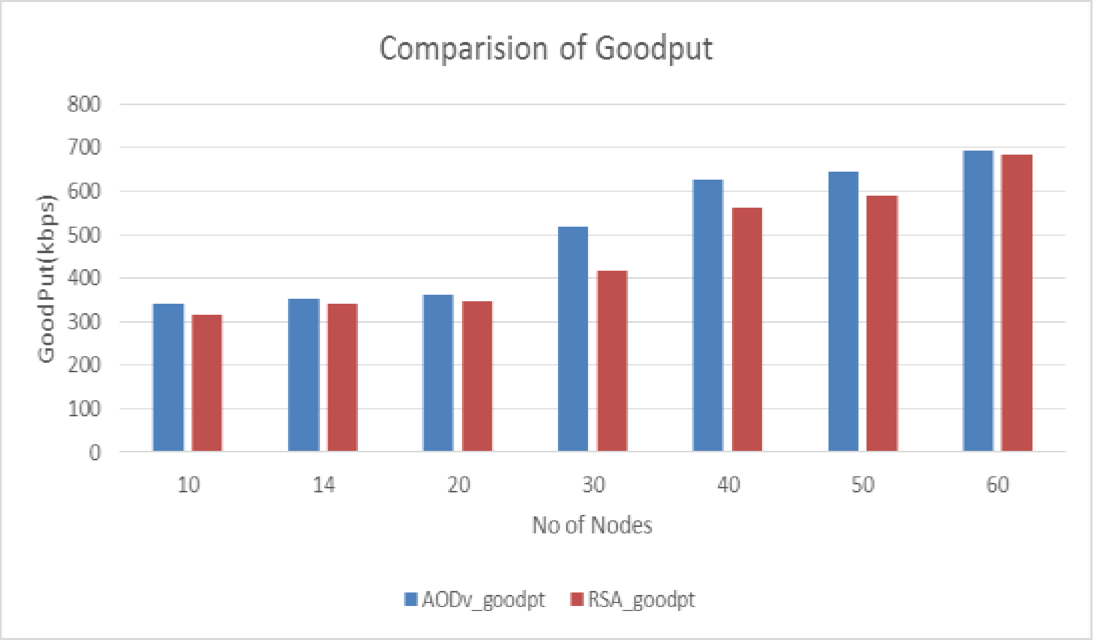

Figure 6: Camparision Goodput graph of AODV and RSA on AODV

VIII. CONCLUSION

As from above scenario it can concluded that the performance of original AODV is good but when we tried to impose RSA on AODV its performance decreases drastically. So there must be protocol which needs to be designed in such a way that it must remove vulnerabilities, increases performance and increases security of exciting protocol that is RSA .So in future proposed work can be such that it increases security and performance of present RSA security and performance.

IX. REFERENCES

[1] Charles Perkins and Elizabeth M.royer “Ad Hoc on demand distance vector routing”, pp: 1-11

[2] Chirag Tehlanl and Divya Sharma“A Study on different security Threats in Mobile ad hoc network”, International Journal of information and computation technology, 0974-2239 Volume 4, Number 1, pp: 1 -10, 2014

[3] Muhammad Saleem Khan,Qasim Khan and Majid Khan “A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks”, Springer-Verlag Berlin Heidelberg, 978-3-662-47669-7, pp: 137-145 Sept 2015

[4] Ashish Sharma,DenishBhuriya,Upendra singh, “Secure Data Transmission on MANET by Hybrid Cryptography Technique”. IEEE International Conference on Computer, Communication and Control, 978-1-4799-8163-2, pp: 1-6 Sept-2015

[5] Ritu partidar and Rupali Bhartiya, “Modified RSA Cryptosystem Based on Offline Storage and Prime Number” IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1594-1 , pp:1-6 Dec-2013

[6] Quing liu,Yunfei Li,Lin Hao and Hua Peng, “Two Efficient Variants of the RSA Cryptosystem” Internation conference on computer designAnd Application”IEEE International Conference On Computer Design And Appliations, pp: 550- 553, 2010

[7] Sisily sibichen and sreela Sreedhar, “An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks” IEEE International Conference on Microelectronics, Communication and Renewable Energy-2013.

[8] Prachi D. Gawande and Yogesh Suryavanshi, “Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's” IEEE ICCSP conference, 978-1-4799-8080-2, pp 1478-1481,April 2015

[9] Sunil J. Soni and suketu D. Nayak "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET" IEEE International Conference on Intelligent Systems and Signal Processing, 978-1-4799-0316-0 pp: 325-328, March 2013

[10] Ali M. Sagheer, "Identity Based Cryptography for Secure AODV Routing Protocol" IEEE 20th Telecommunications forum TELFOR, 978-1-4673-2983-5, pp: 198-201-Nov 2012

[11] http://perso.crans.org/raffo/papers/phdthesis/thesisch1.html