Routing Algorithm using DNA Cryptography in MANET

Sonam Modi
M.E. Computer Science and Engineering,
GEC Gandhinagar, India

Abstract **- MANET is collection of nodes with wireless communication and networking capability that communicates with each other without any centralized node as it is infrastructure less. Due to mobility and limited radio range, every node has to perform the dual responsibility of host of different services as well as routers for forwarding information. Different routing algorithms are used for transmitting the information such as DSDV, DSR, AODV. In MANET communication is done via open medium, so Transmitted information and network is vulnerable to different types of attacks. Thus, for providing security against unauthorized access to data there is need for secure routing protocols.DNA Cryptography is used to safeguard the data against the unauthorized access. We consider protocol AODV i.e. Ad-hoc On-demand Distance Vector.DNA cryptography is used in routing algorithm of MANET as security has always been main concern in data communication and networking.DNA cryptography as an approach to ensure highly secure environment for transmission of data across mobile networks. The DNA cryptography is used in routing algorithms which reduce the impact on security of MANET.**

Keywords **– MANET, Routing protocols, security, DNA Crytography**

I. INTRODUCTION

Mobile ad hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as a service host and a router for all other nodes in the network.

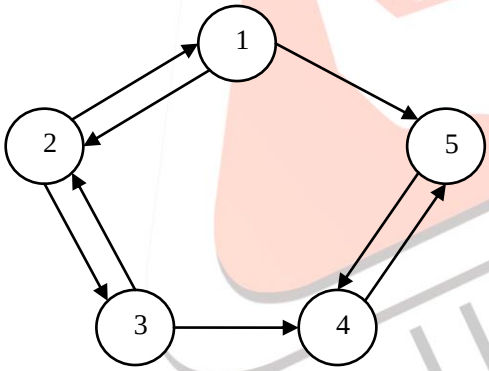

Fig 1 Mobile ad hoc network [1]

Mobile Ad hoc Network (MANET) is a collection of mobile nodes that are arbitrarily located so that the interconnections between nodes are dynamically changing. Some links are symmetric which work in both direction and others are asymmetric which work in only one direction. Mobile Ad-hoc networks are composed of autonomous wireless nodes i.e. it requires no central node to manage the networks .All the work is done with the mutual agreement and understanding between the nodes. Thus every node has to perform dual responsibilityof host and router. Because of mobility nature of nodes, topology of the network changes with time and makes the ad-hoc network to be a non–infrastructure network. Every node has the self configuring ability.

In MANET, each node acts both as a router and as a host & even the topology of network may also change rapidly. Some of the challenges in MANET include:

1) Unicast routing
2) Multicast routing
3) Dynamic network topology
4) Speed
5) Frequency of updates or Network overhead
6) Scalability
7) Mobile agent based routing

8) Quality of Service
9) Energy efficient/Power aware routing
10) Secure routing

II. AODV ROUTING PROTOCOL

Routing protocols in MANETs may be classified into following categories:

- Proactive (table-driven) routing
  - DSDV
- Reactive (on-demand) routing
  - AODV, DSR, TORA
- Hybrid (both proactive and reactive) routing
  - ZRP

AODV Protocol Description [3]

AODV Ad–hoc on demand distance vector routing (AODV) is a stateless on-demand routing protocol. The Ad-hoc On Demand Distance Vector (AODV) classified under reactive protocols. The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. The operation of the protocol is divided in two functions, route discovery and route maintenance.

AODV Routing Mehanism

Path discovery:
Every node maintains two separate counters
- Sequence number
- Broadcast-id (increments whenever the source issues a new RREQ)

Path maintenance:
- Neighboring nodes with active routes periodically exchange **hello** messages
- If a next hop link in the routing table fails, the active neighbors are informed.

III. DNA CRYPTOGRAPHY

Security services include the functionality required to provide secure networking environment. The main security services are: Authentication, Confidentiality, Integrity, Access control, Availability

A. Various Attacks in MANET

- Passive attack: A Passive attack does not disturb the routing protocol operation, but only tries to find valuable information by listening to routing traffic, so it is very difficult to detect.
- Active attacks: An active attack is an effort to alter the data, authentication gain, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Active attacks are- Impersonation, Modification, Fabrication, Denial of service,

B. DNA Cryptography Description [2]

- Security has always been the main concern in data communication and networking. Mobile Networks are highly vulnerable to security attacks and pose a great challenge for the wireless networks being used today
- DNA stands for Deoxyribonucleic acid which store genetic information of the entire living organism ranging from human being to small viruses. It is also called as an information carrier and consists of long polymer of small units called nucleotides. Further nucleotides consist of three components: Nitrogenous base, five Carbon sugar and Phosphate group. Nitrogenous base consists of four bases: Adenine, Thymine, Cytosine and Guanine (A, T, C, G), all the complex information about organism are stored with the combination of these bases. Adenine and Guanine are called purines, whereas Thymine and Cytosine are called pyrimidines.
- Pseudo DNA cryptography approach which, is based on the central dogma of molecular biology. Concept of how messages are stored in DNA and then transfer to the mRNA (transcription), and then to the proteins (translation) which is our ciphertext. Ciphertext is send through the secure channel to the intended receiver and symmetric key with one-time pad is used at both the ends (encryption and decryption).

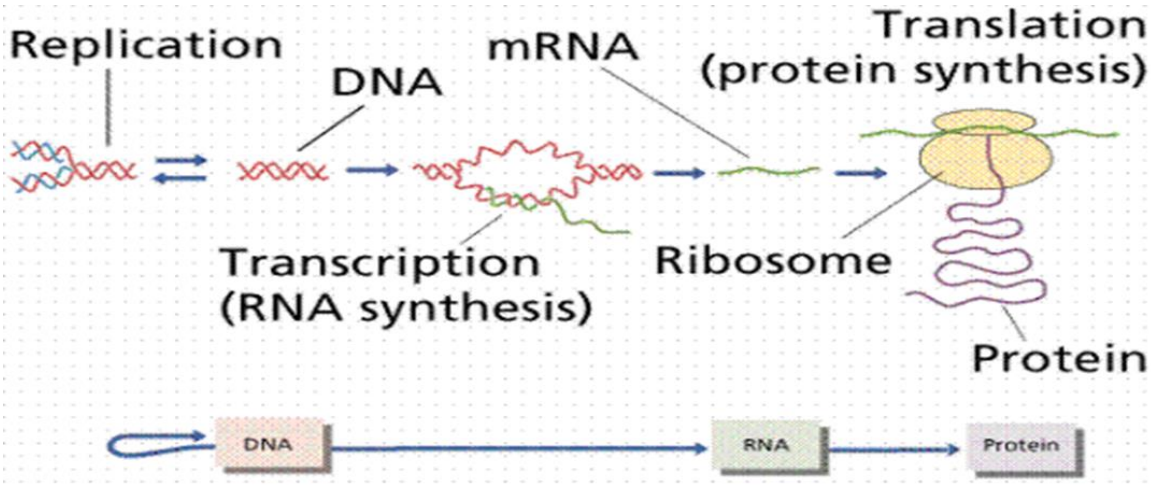

Figure 2 . The Central Dogma of Molecular Biology [4]

C. Advantages of DNA Cryptography

- Does not use DNA sequence but use mechanisms of DNA functions.
- Uses central dogma of molecular biology.
- Powerful against attacks like brute force attack.
- Efficient in computation.

Encryption and decryption time is affordable in MANET by use of DNA cryptography.

IV. Proposed Modified AODV Protocol

We modify the AODV to take into account the pseudo DNA cryptography method, based on central dogma of molecular biology. The proposed protocol is based upon pseudo DNA cryptography method using one-time-pad. This method is powerful against certain attacks, especially against brute force attack. This algorithm provides integrity, non repudiation and confidentiality.

A. Performance Metrics

- ✓ **Packet delivery ratio:** the ratio of the number of delivered data packets to the destination and number of packets send.
- ✓ **Routing overhead**: how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.
- ✓ **Energy Consumption:** When a node sends or receives a packet, the networks interface of the node, decrements the available energy.

B. DNA cryptography Encryption and Decryption

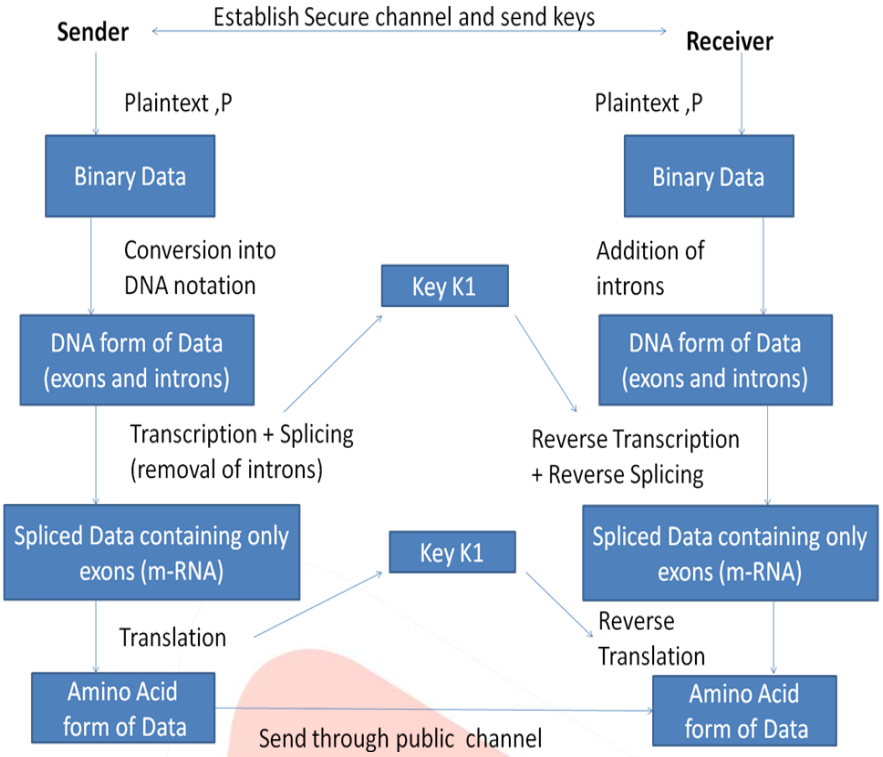

Figure-3. DNA cryptography Encryption and Decryption [2]

As shown in figure-3 this algorithm is used in AODV routing protocol for improving security in MANET.

C. Flow of proposed work

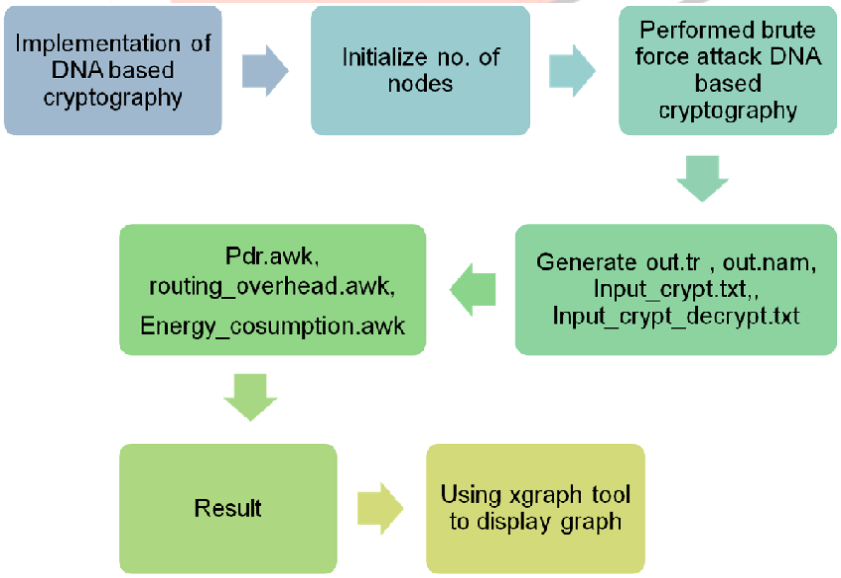

Figure-4 Proposed work

D. Parameters checked against

Parameters	Value
Number Of Nodes	50
Simulation Area	1050*600m
Transmission Range	250m
Speed	4 packets/sec
Node Mobility	10 (mps)
Data Packet Type	CBR
Packet Size	512bytes
Data rate(mbps) mobility model	Random Way Point

E. Simulation Results

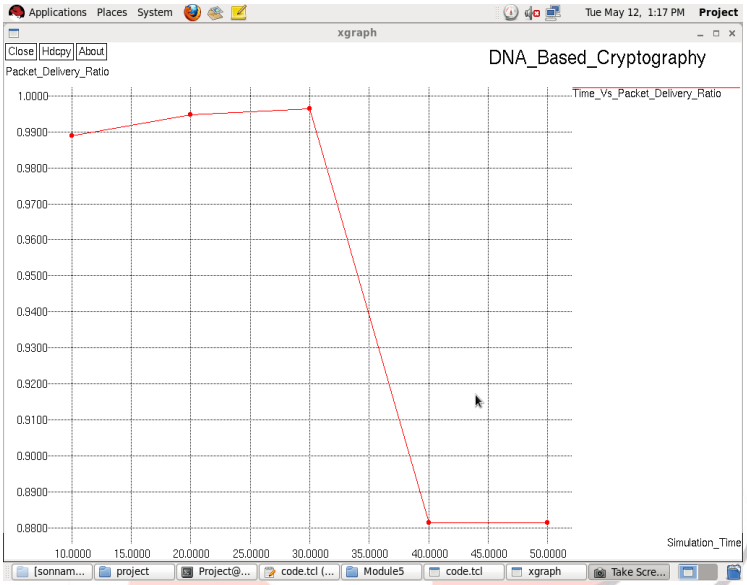

Figure-5.Time versus Packet Delivery Ratio

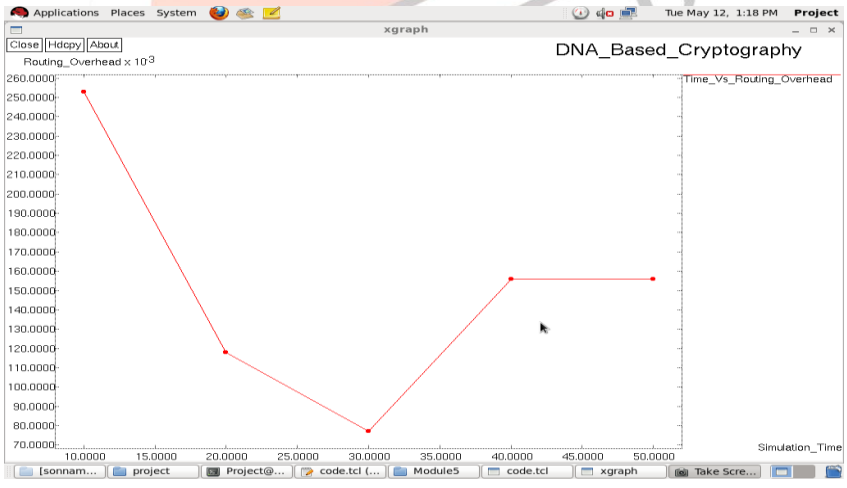

Figure-6.Time versus Routing Overhead

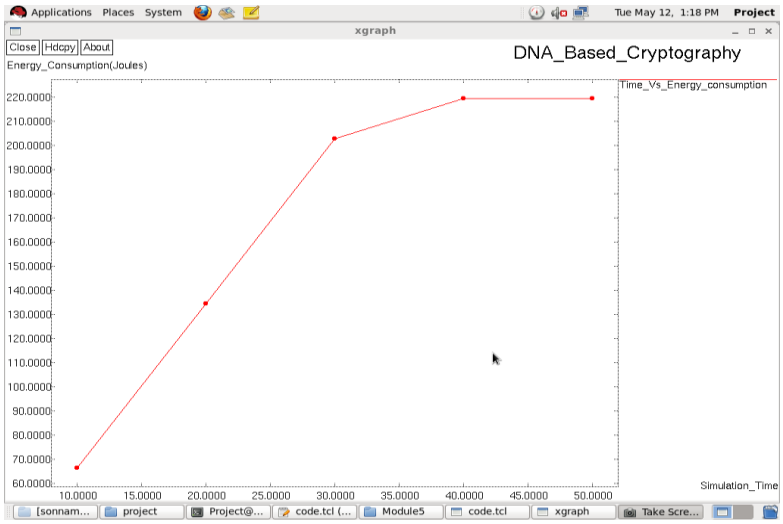

Figure-7.Time versus Energy Consumption

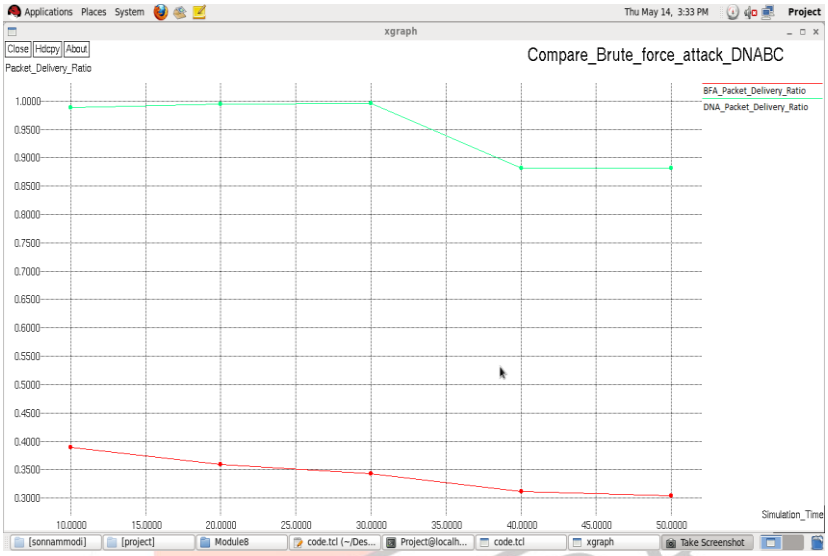

Figure-8.Time versus Packet Delivery Ratio – comparison

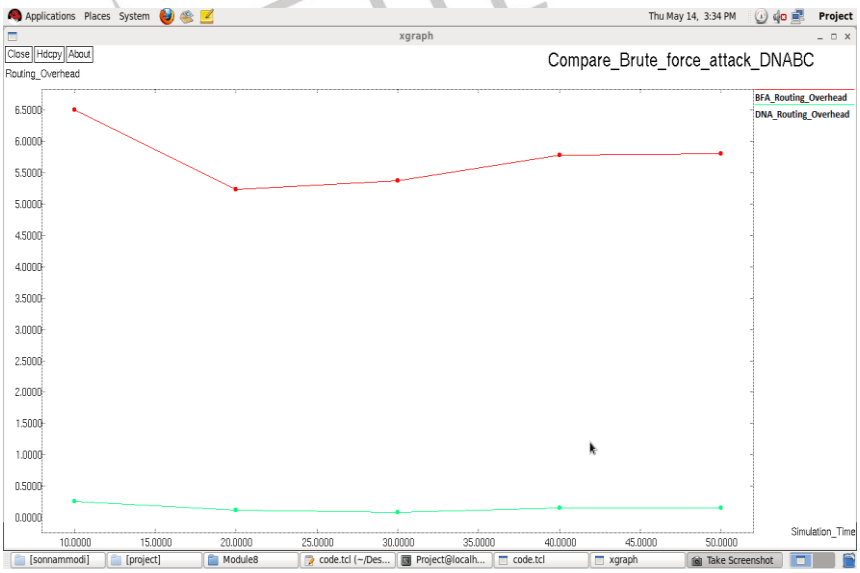

Figure-9.Time versus Routing Overhead – comparison

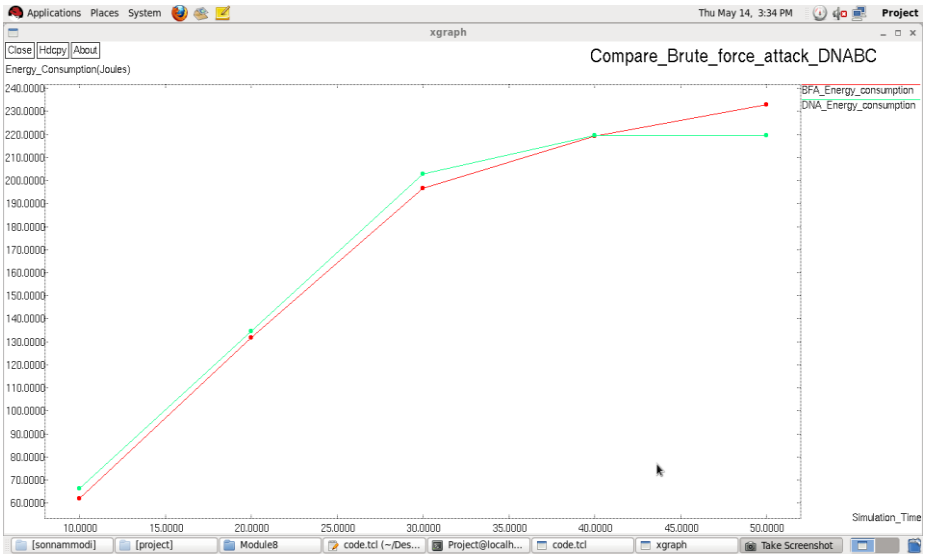

Figure-10.Time versus Energy Consumption – comparison

F. Performance matrices

	Cryptography	DNA cryptography
Routing overhead	21.405	0.150
Packet delivery ratio	0.1039	0.8808
Energy consumption	58.8513	219.44

V. CONCLUSION

In Mobile Ad hoc network, Routing security is a major issue as routing protocols have no built in security mechanism. In this report, we explain the basics of MANET with its characteristics, routing and various attacks that compromise the security of network. We modify the AODV algorithm to take into account the pseudo DNA cryptography method. The proposed protocol is based upon pseudo DNA cryptography method using one-time-pad in MANET.

In future enhancement, we can implement Geographic-distance-based Connected-K neighborhood for First path (GCKNF) sleep scheduling algorithm in DNA based cryptography Network to increase the network lifetime.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Department of Information Technology(INTEC), Belgium

[2] Harneet Singh, Karan Chugh, Harsh Dhaka, A. K. Verma"DNA based Cryptography: An Approach to Secure Mobile Networks" *International Journal of Computer Applications (0975 - 8887)* Volume 1 – No. 19, 2010, page(77-80)

[3] Aarushi, Harish Bedi, "A Review on Attack in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 4, Issue 7, July 2014,page(794-798)

[4] Rupali Soni, Gopal Prajapati," A Modern Review on DNA Cryptographic Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 3, Issue 7, July 2013,page(162-167)