Routing Attacks Detection and Preventive Measures in Mobile Ad-Hoc Wireless Networks using An Effective Method of DNA Based Cryptography

M.Jhansi[1], Dr. M.Balraju[2]

Research scholar, JNTU Hyderabad[1], India
Principal [2]Swami Vivekananda Institute of Technology, Hyderabad, India

Abstract. MANETs faces different security threats that is attacks which are carried out against them to disrupt the performance of the networks. In MANETs the nodes themselves act as routers. Routing attacks are the one generated in network layer in this paper my work focus on the detecting attacks those nodes which misbehaves leads to attack and preventing measures by providing cryptography security measures to forward data packets without loss or dropping in the network. Whatever the existing system using Intrusion Detection system mechanism uses an alert message in order to identify an attack every time this is a time consuming process and every time routing table change detector needs changes in the routing table in order to avoid these drawbacks in this paper an effective mechanism has been implemented to detect and prevent routing attack in MANET. The proposed solution shows various routing attacks detection and prevention in the network with simulation. Proposed protocol has been simulated using NS2 simulator environment. The simulation results shows the efficiency of its performance.

Keywords. Routing Attacks, Detection, Prevention, MANET.

1 Introduction

MANET are vulnerable to many Routing attacks[4] in a network to diminish and eliminates a network by various misbehaving actions to function. Before the development of any security measures it is important to study the variety of routing attacks. In this paper a node which is called as intelligent node proposed to distribute the key to each node in a mobile ad-hoc network environment to avoid attacks. At the time of network formation itself each node is well aware of the key in the network. Routing attacks like sleep deprivation, route salvage and colluding miss relay attacks are significantly reduced with the proposed schema. There are some existing intrusion prevention measures will be there but the mechanisms used either causes greater overhead and latency and sometimes they cannot defend against malicious internal nodes.

2 Existing work

There are many existing approaches like Dempster-shafer theory[2] has been given a solution for routing attacks where the rule of Dempster used to mitigate the routing attacks. And there is an Intrusion Detection System mechanism uses the creation of message when the attacker attacks the network which gives an alert message to each node in the network. Even in other methods like trusted based mechanism due to the lack of trusted environment in an ad hoc network results in many security lapses and this is considered as one of the major concerns in the large scale deployment of ad hoc networks. Many trust establishment algorithms have been developed. Traditionally used mechanisms such as authentication and encryption methods are not capable to handle some kind of attack such as packet dropping by malicious nodes in the MANET environment. Existing techniques uses clustering type of architecture to monitor and prevent attacks but it is only localized one. This localized and distributed behavior reduces the bandwidth utilization.

3 Proposed Detective Preventive Method

This section gives the proposed method to detect misbehaving nodes under attacks. Our proposed mechanism uses a reputation data management calculated reputation rating of each node. Reputation in MANETs is defined as how good the node is interms of its contribution to routing activities in the network. Malicious node is detected by utilizing the concept of reputation. When a node joins the network the reputation value is given to be 1 this is called initial threshold value. The reputation value of a node updated based on information received from neighbors both for data discovery and exchanging mechanism. Each node maintains and broadcasts its rating similar to routing information exchange. If service is needed by a neighboring node it gives it a successful service indicated as S between the nodes it rates it as a positive value 1 and the services it does not need it gives it as unsuccessful service which is represented as U with negative value -1. Reputation data is computed as the sum of ratings of the individual services of each node. We considered the node which is giving service successful is the node involved in the route discovery process and those nodes which is not giving its service is identified as malicious nodes under attack. This reputation data which is having higher reputation value which we call the node as an intelligent node. The node which is identified below the pre-defined threshold value as malicious. Not only the detection of malicious nodes we need to give a secure transfer of data delivery between source and destination, for that an

intelligent node is selected to distribute a key to the nodes involved in the route discovery because key distribution is the major problem. Authentication is provided by giving a Hybrid DNA based cryptographic Mechanism to preventing routing attacks. This mechanism is mainly used for achieving data integrity and confidentiality.

3.1 Assumptions

The following are the assumptions for the proper operation of the proposed schema (1) Each mobile node in the network has a unique ID which can join and leave the network freely.

(2) Initially, each node is having equal computational and storage capability

(3) Maintaining reputation data among the nodes is correct and there is no collusion among nodes.

3.2 Proposed Architecture

Algorithm:

Sender encrypts the plain text using symmetric key into DNA sequence and sends through the intelligent node to neighbouring nodes.

Sender→ $E(K_{dna}, P)= C_{dna}$

Receiver decrypts the cipher text into plain text using DNA key sequence.

Receiver→ $D(C_{dna}, K_{dna})= P$

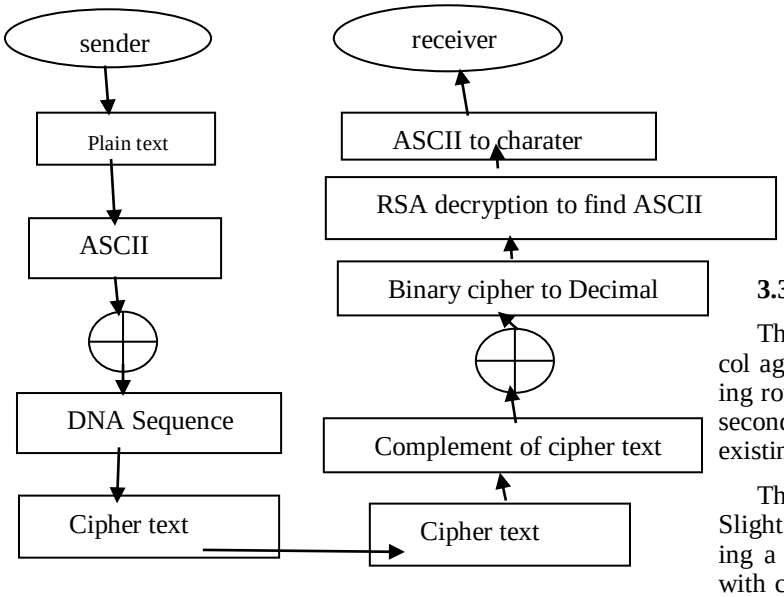
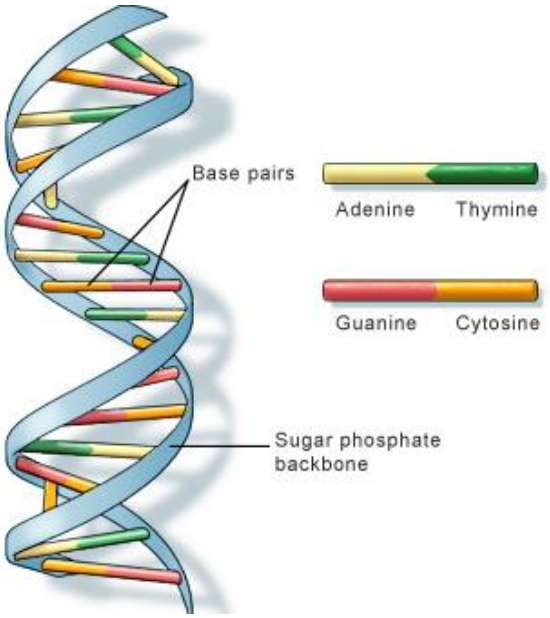


Fig 3.2.1 DNA based crypto system model

The source node wants to send data to the destination it initiates route discovery process by broad casting a message Route Request packet with a DNA secret key based on DNA cryptography with its neighbor nodes until it reaches to the destination

DNA contains double hydrogen bond with (A, T) and (C, G) which are complement to each other. Deoxyribonucleic acid is a molecule called nucleotides. Each nucleotide is made up of one of four nitrogen-containing nucleobases — cytosine (C), guanine (G), adenine (A), or thymine (T) — a sugar called deoxyribose, and a phosphate group.



This illustrates the structure of DNA, with strands holding the base pairs. Image by U.S. National Library of Medicine.

Nucleotide	A	C	G	T
Code	00	01	10	11

Fig3.2.2 Binary codes

3.3 Secure Routing Protocol: SRPARA

The proposed Protocol is SRPARA (secure routing protocol against routing attacks) handles two issues, first is detecting routing attacks against AODV in wireless adhoc network, second is integrating DNA based cryptographic approach into existing AODV routing protocol.

The proposed work modifies the original AODV protocol. Slight modification is done at destination node by broadcasting a message Route Reply packet back to all its neighbors with current route until it reaches to the source node to create multiple route instead of unicasting in original AODV protocol. Multiple paths between the source and destination nodes can be used for two purposes. First if at all the primary selected path is fail to send packets to the destination. Second after detection of malicious nodes, source node will direct the traffic with alternate route to the destination. Finally the routing path is selected based on the reputation database with neighbor

ratings which are not conformed having malicious behavior will be eliminated from the route.

3.4 Experimentation Results

3.4.1Sender side Algorithm:

Suppose sender wants to send 'I love india' to receiver. So size of plaintext=12

Step 1: Sender generates a random binary key of size=8*size of plaintext. So for this plaintext it becomes =96.

Let it is: 1 1 0 1 0 1 1 0 0 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 1 1 1 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 1 0

Step2:

Sender convert plaintext to its corresponding ASCII value then apply RSA to each ASCII value by RSA key to find out RSA cipher.

Step3:

Sender converts each digits of RSA cipher to binary plaintext of 8bits.

Now the length of binary cipher becomes 8*length of RSA cipher

Step4: perform XOR operation with binary cipher and random binary key

Step5: convert result into DNA sequence by using the following algorithm

1.Begin

2: DNA patterns

Assign the 2-bit patterns of Binary String to convert in to DNA SEQUENCE

4: for (i ⇐ 0 to stringlength do +2) do

if (String Cmp(Binary,"00") ==0) then

6: DNA-Code[i]⇐ 'A';

else

8: if (String Cmp(Binary,"01") ==0) then

DNA-Code[i]⇐ 'C';

10: else

if (String Cmp(Binary,"10") ==0) then

12: DNA-Code[i]⇐ 'G';

else

14: if (String Cmp(Binary,"11") ==0) then

DNA-Code[i]⇐ 'T';

16: end if

end if

18: end if

end if

20: end for

End

The above code is converted to the cipher text format

TCCGAATTCCCCTTATGTCGTCTGCGAAGAAAAAC-CAAAAATGAGAAG

Step6: complete DNA cipher is generated and is given to the intelligent node inorder to avoid routing attacks

The node then distributes the key to the route discovery nodes but the receiver only have the decrypts the message by using following steps

3.4.2 Receiver side algorithm:

Step1: the cipher text message is first converted to complement cipher text

Step2: receiver performs XOR operation between binary key and cipher text to find binary cipher

Step3: now convert every 8binary cipher to its corresponding decimal number

Step4: decrypt each decimal by RSA decryption key to find ASCII value then convert to its corresponding characters then it becomes 'I love india'

4 Performance analysis

The effect of performance of the misbehaving nodes, network size,pause time,and simulation time were investigated using following parameters

Parameters	Values/ranges
Simulation Area	1000 x 1000
Speed(m/s)	1 m/s or 20 m/s
Packet Rate	5 Packets/s
Packet Size	128 bytes
Traffic source	CBR
Pause time	Uniformly distributed
Routing Protocal	AODV
Number of Nodes(max)	100
Transmission range	250m
Simulation time	900s

Measures are Average packet delivery ratio, detection rate, routing overhead and misbehaving node detection rate.

5 Conclusion

In this paper, an efficient way mechanism is implemented to detect and prevent routing attacks Manets. The proposed system gives the solution to find malicious nodes which acts like a malicious behaviour node in the network to which is not cooperatively operated in the network. The prototype of the algorithm is implemented in Matlab. In this paper a new text encryption technique based on DNA[6] and RSA is implemented to ensure high security in two levels. It is a hybrid approach which combines the idea of symmetric and asymmetric cryptosystem. Thus, it ensures more security than those processes which used symmetric cryptosystem. But in this paper, when ASCII values are encrypted by RSA, we limit our ciphertext size is multiple of 8 bit. This is the limitation of the system. In future, this limitation will be tried to be solved. Also, the random binary key needs to be shared between sender and receiver. So, how securely the binary key shared between two parties is also a future concern.

References

1. N. Song, L.Qian, X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", Parallel and Distributed Processing Symposium, Proceedings, 19th IEEE International, 2005.
2. Zawtun and Aung Htein Maw, "Wormhole attack detection in wireless sensor networks", World Academy of Science, Engineering and Technology, 46, 2008.
3. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons. Inc., Chichester (1996).
4. Kannhavong, B. Nakayama, H. Nemoto, Y. Kato, N. Jamalipour, A , "A survey of routing attacks in mobile ad hoc networks", IEEE Journal on Wireless Communication, Vol-14, Issue 5, December 2007, ISSN: 1536-1284, pp.85-91.
5. Marti, S.Giuli, T.J.Lai,K.Baker,M:Mitigating routing misbehavior in mobile adhoc networks, In:Mobile computing and Networking.(2000) 255-265
6. Shreyas Chavan: DNA Cryptography based on DNA Hybridization and One Time Pad scheme, International Journal of Engineering Research & Technology, Vol. 2, Issue 10, October 2013, pp. 2679-2682.