ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Prevention from Black Hole Attack Using RSA Algorithm

[I]Gaurav Dwivedi, [II]Manveer Kaur
[I,II]School of Computer Science, Lovely Professional University, Punjab, India

Abstract
The black hole is a kind of security attacks that mostly perform in mobile ad hoc networks (MANET). Main problem in MANET is that it does not have fixed infrastructure, they have dynamic components which regularly change as place to place. Here in this paper we will discuss some routing protocols which used in MANET , and also going to describe our proposal work " prevention from black hole attack using RSA algorithm". So one question firstly strike in minds why we chose RSA. Let me tell you RSA is the one of the best cryptographic algorithm for encryption and decryption. we will further discuss RSA with our proposal work.

Keywords
AODV, MANET, RREQ, RREP, RSA.

I. Introduction

In wireless system more security is needed comparison to wired networks. In wireless network where a term MANET(mobile and ad hoc networks) comes , there exist some harmful attacks like black hole attack, gray hole attack and wormhole attacks are possible. Here we are going to prevent black hole attacks[1]. Black hole node draw a confusion to a source node that he is the node who deserve to receive the packets, and the data will be send to blackhole node.. Lots of algorithm or cryptographic techniques used to prevent black hole node. We will further describe it but in our work we are going to use RSA. That is one of the best security algorithm used in cryptography. MANET use some routing protocols . which helps to rout the data from the suitable path. Basically there three type of routing Protocols[2].

1. Table-driven Approach or Proactive routing Protocols.
2. On-demand Approach or Reactive routing Protocols.
3. Hybrid Routing Protocols

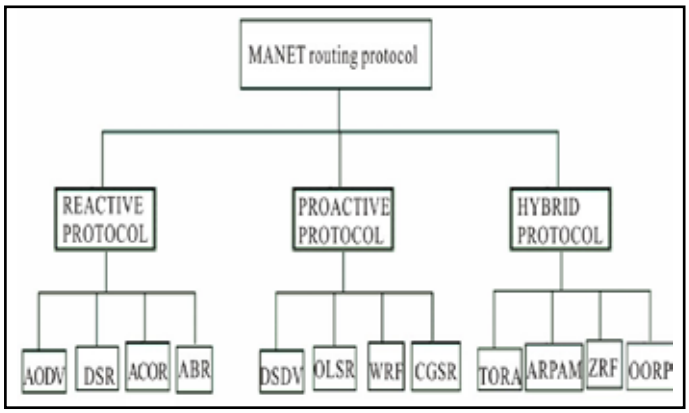

Fig. 1: Routing protocols of MANET

Table driven: in this type of protocol each and every mobile nodes contains a table , which maintains the routing information in table. After a time period, it updates the information in the routing table, if any updation needed. Updating process run continuously and helps to provide a better shortest path. DSDV ,WRP protocols comes under this category.

On demand routing protocols: In this type of routing technique the mobile nodes does not maintain any routing table.

It is source initiated protocol. The route between source and the destination is finding only when source node want to communicate with other node, shortest one selected. The route request is generated dynamically and the route response is also. Instead of maintain a routing table every node maintains a route a cache. DSR ,AODV, TORA protocols comes under this category.

Hybrid routing protocols: These types of protocols are simply the combination of the protocols. They combine the best feature of the both protocols, Table-Driven and On-Demand . ZONE routing protocols is the best example of this category.

B. Black Hole Attack

In the below diagram there is a Source node 1 want to transfer the packets to the Destination node 4, other nodes are intermediate nodes. First of all source node send the route request for sending the packets, that is called RREQ[3] . When intermediate nodes receive RREQ than they will send reply of request, that is called RREP. After the collecting of RREP from all the nodes, than it will send the packets based on their heights sequence number. Sequence number would generate on based of its algorithm which previously saved in nodes. So source node will send the packets to the node having highest sequence number. The node which receive the packet it further transfer to other nodes , by this way packet should be reach up to the destination , but not necessary it should happen all the time. Sometimes a black hole node come into existence which only receives the packet and not transfer it further to any other nodes. That node is called black hole node , and this attack is called black hole attack[4].

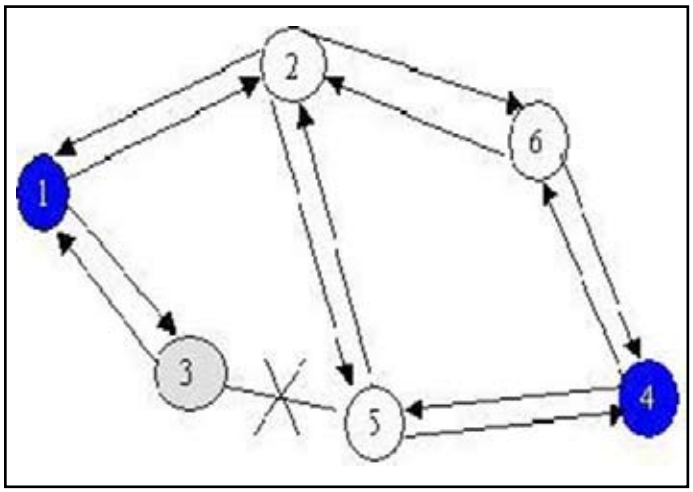

Fig. 2: Example of black hole attack

In the above diagram we can watch node 3 is black hole node which further not transferring data to any other node.

© 2013, IJARCST All Rights Reserved

III. Literature Survey

Honmei Deng Wei Li, and P.Agarwa creates a method for detection of the black hole node. In that intermediate node send the information to the next hop while it sending back to an route reply message. When source receive RREP through other nodes .Firstly it takes time to gaining knowledge about the next hop information, instead of sending the data packets at now and then send forward its request to the next hop for confirming that it has the suitable and secure route from the intermediate node. If the next hop does not have any route to the intermediate node, but has a perfect route to the destination node, than it will discard the reply packet receive from previous node, and start searching for new route.

Satoshi Kurosawa , Hideshia Nakayama , Nei Katao propped a new method, according to him when the black hole node will receive RREQ from source node, than obviously he will try to send the RREP greater than destination node. So for that attacker need to find the highest sequence number present in the network, so any legal node will not try this, only black hole node or malicious node will perform this type of action. So they able to catch blackhole node by help of these algorithms.

Payal N. Raj and Prashant B. Swadas proposed DPRAODV (detection, prevention and reactive AODV) it will also help to find the black hole node well as inform the other nodes about the malicious node or black hole node. They actually set a threshold value on receiving reply packets. If the number of RREP packet is more larger than the defined threshold value than it will be add in blacklist , considering it is black hole node, being a black hole it will try to send RREP as per as maximum value and may be cross the threshold value. After adding the node in blacklist they send alarm to the other nodes about particular node.

E.A.Mary, Anita proposed also prposed a digital signature scheme, kind of issuing a particular certificate of each node . node shares this certificate to other nodes which are in range of particular radio transmission . and also a unique certificate send to each node by the source node as a digital signature. There is a chance of certificate confliction cause one certificate should issue by the sender and the other will be generate periodically , confliction means , something is going wrong.

Amol Bhosle proposed an efficient solution for the prevention of the Black hole nodes in the Mobile and Ad hoc networks based on the AODV routing protocol. In this algorithm, known as Modified AODV mechanism a Watchdog mechanism is used. On that mechanism each and every node maintains two extra tables. First one is named as Pending Packet Table and another table is known as Node Rating Table. First table contains Packet ID, Next Hop, Expire Time and Packet Destination while the Node Routing Table contains Node Address, Packet drops, Packet forwards and Misbehave. For the communication each and every node listens to those packets that are within the communication range of that particular node threshold value is used for the detection of whether node is malicious or not and also a node can repair all the nodes locally which contain the malicious node.

M. Umaparvathy proposed a new protocol called as TTSAODV Protocol to identify single as well as collaborative black hole node in MANET. This protocol verifies the trueness of the route reply message through the Verification messages sent by neighboring nodes. The basic assumption on they provide two strong level. In actually ,a pair of nodes contains a unique secret keys which will share among them of concepts one is while route discovery while the other one is during data transfer So, the proposed protocol has high level of degree of attack detection and prevention.

Hesiri Weerasinghe proposed the work which discovers the corporating black hole nodes .its actually a generalized version of other previously used algorithms. They actually divided the node into the several groups ,[5] than cross check it as group voice. This technique is not much new, because this was the same as AODV protocol in which it introduce by data routing or DRI .table and after that it checks on based of the Further Request(FREQ), and Further Reply(FREP), containing some changes makes it better than previous one.

IV. Proposal Work

A. Firstly we take 6 nodes n1 ,n2 ,n3 ,n4 , n5 , n6 and also a authentication an.

B. Every node will chose unique number and send to an. An will tell them the that the number is unique or not.

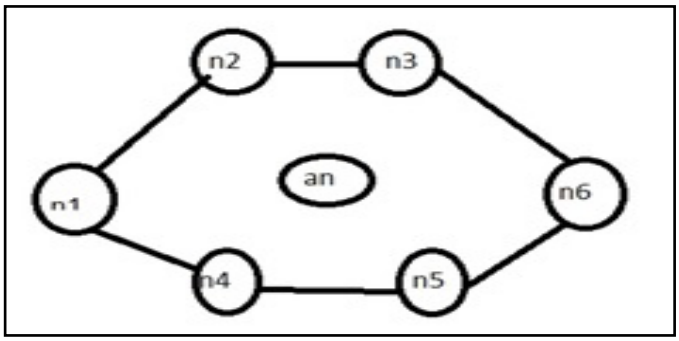

Fig. 3: nodes

C. Now an will store all unique number.

D. Chose source an destination.

E. Source node will request for unique number through source to destination with the help of RREQ.

F. Destination node will send RREP packet with unique number.

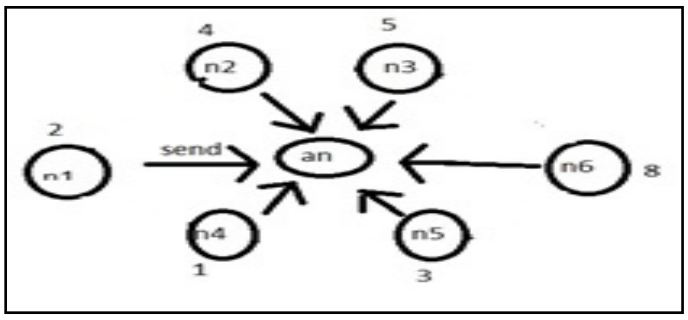

Fig. 4: Sending unique numbers

G. Now source node will verify unique number from an node. Now main point it will verify the unique number which is received same from number of paths.

H. Now after sender unique number destination node will set timer on it. Timer will start from 10 sec to 0 sec and in between these 10 sec, it will not get data than it inform to source node through all possible paths.

I. Now the source node will encrypt data using modified RSA.

J. As per first step of RSA we have to choose two unique prime numbers and this number will be chosen as same we chosen earlier.

K. Now the message of that node is going to exchange were exchanging through image pattern.

© All Rights Reserved, IJARCST 2013

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

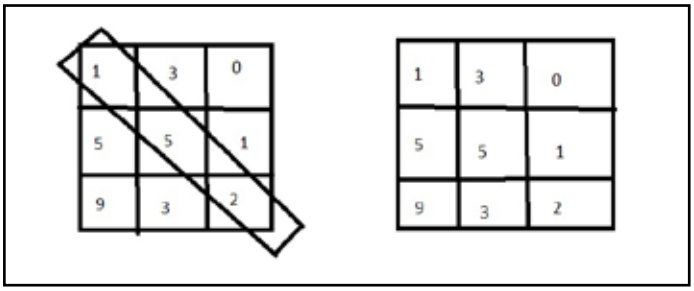

Fig. 5: Image pattern

So here the total number is pattern is 1+5+2=8
Here is particular flow chart for that, take a look .

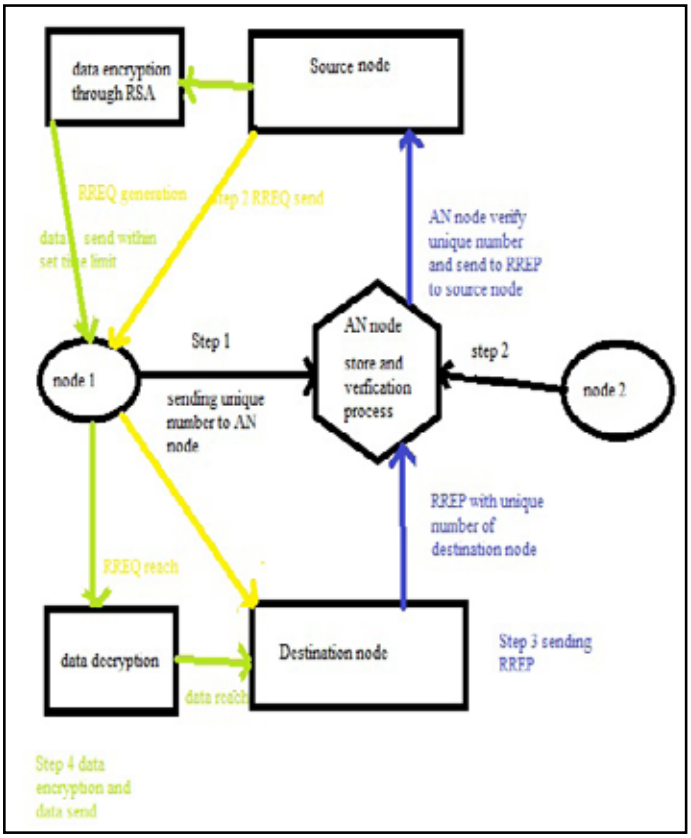

Fig. 6: Diagram representation

Now , how the data will be encrypt through using RSA, let's take a look of steps of RSA algorithm.

1. Select the value of p and q , that must be unique prime number.
2. Then multiply p, and q, and calculate n
3. Further calculate phi n=(p-1)*(q-1)
4. Select the value of e as similar as p, and q,
5. Find the value of d by d=e^-1 (mod(phi n))
6. After that we are sender node will perform encryption by c=M^e mod n
7. Same as decryption process will perform at the destination node side the data by M=c^d mod n Where C is encrypted text M is the message on which both process of encryption and decryption will be performed encrypt. The value of p, q, e should be chosen by the sender[6].

V. Conclusion

Security is the important issue of routing protocols of MANET. In AODV routing protocols , nodes having highest sequence number is selected for fresh and short route. In black hole attack malicious node will accept RREQ from source node and drop the packet instead of sending to the destination. MANET creates dynamic topology[7]. Main problem of dynamic topology it varies on regular basis, there is no fixed infrastructure. The nodes of these type of networks find or search the route dynamically when a node want to communicate with other nodes and thus use adaptive or dynamic routing, for this mostly prefer dynamic protocols . they networks are showing significant importance into many real life and home applications such as military applications medical uses etc.

In our research paper we prevent the black hole attack using RSA algorithm. This proposed approach is used to detect the black hole node and prevent cooperative black hole attack. I also used to terms of unique numbers which is totally new concept in MANET that provide a better and unique way for better authentication, which tells that number come from which node, node is verified or not. By using RSA we give a better cryptographic technique, which sends the packet in encrypted form, by the way if attacker bypass the unique number technique after that it has no chance to read the data cause of its in encryption form[8].

In future work we can see more cryptographic algorithm to prevent such attacks cause encryption is the best from where a sender can securely send the data to the receiver without tension. Cracking the encrypted data is tuff task and if it is encrypted by large unique primary value, than the task became like impossible[9].

Refrences

[1]. *Ayesha Siddiqua, Kotari Shridevi ,Arshad Ahmad Khan [2015]." Prevention black hole attack in MANET using secure knowledge algorithm " in" SPACES 2015".*

[2]. *Ms. NIdhi sharma, Mr. Alok Sharma[2012]" The black hole attack in MANET "Institute of Electrical and Electronics Engineers(IEEE)" page no. 125-128 vol 17.*

[3]. *Xiong Kai, Yin Mingyong Jiang Hong [2015]," A Rank Sequence Method For Detecting Black hole In Ad hoc Network" "International Conference of Computing and Internet of Things "(ICIT) 2015 vol 7 Page no 32-36.*

[4]. *Pooja, Dr. R.K.chohan [2014] " An Assessment based approach to detect black hole attack in MANET" in "International Conference of Computing , Communication and Automation "(ICCCA) vol 6 Page no 120-124.*

[5]. *Mehdi Medadian, Khossro Fardad [2014]" Modified AODV Protract from Black hole Attack" in International Journal of Computer Science and Security" (IJCSNS) volume 14 no 3 march 2014.*

[6]. *T.Manikandan , C.Senthilkumar ,"Removal of Selective Black hole Attack in MANET" in "International Journal of Innovative Research in Science , Engineering and Technology(IJIRS)" vol 3 , march 2014.*

[7]. *Loay Abusalah Mohsen Guizarni " A Survey of Security Mobile Ad Hoc Routing protocols" in IEEE communication . Vol 10 pp. 7894 , 2008.*

[8]. *Ira Nath and Dr. Rituparma chaki [2013] "A New Blackhole Attack Prevention System in Clustered MANET" in "International Journal Of Advanced Research In Computer Science And Software Engineering(IJARCSE)" Vol 8 Page 73-77.*

© 2013, IJARCST All Rights Reserved

[9]. Romina Sharma and Rajesh shrivastav [2014] "Modified AODV Protocal to Prevent Blackhole Attack in Mobile Adhoc Networks" in "International Journal Of Computer Science And Network Security(IJCSNS)" Vol 11 Page no 63-68.

[10]. Ankit V. Ranchh and yatin v.shukla [2015] "A Noval Approach for Detection of Blackhole Attack" in "IOSR Journals Of Computer Engineering(IJCE)" Vol no 8 Page no 97-101.

[11]. Bhoomika Patel and Khushboo Trivedi [2013] "Prevention and Detection of Black hole Attack in AODV based on MANET" in "International Journal Of Computer Science And Information Technologies(IJCSIT)" Vol no 10 Page no 122-117.

[12]. J Arshad and M Aazad " performance evaluation of secure on demand routing protocols for mobile ad hoc networks" in IEEE communication vol 13, pp. 972-974.

© All Rights Reserved, IJARCST 2013