Cryptographic Approach to Overcome Black Hole Attack in MANETs

Mohan Kumar S B
PG Scholar, Department of ECE, REVA ITM, Bangalore, India.

Nirmal Kumar S Benni
Asst. Professor, Department of ECE, REVA ITM, Bangalore, India.

Abstract - MANETs (Mobile Ad hoc Networks) are De-Centralized wireless networks with Self-configuring mobile nodes. Due to the absence of trusted centralized authority or openness of network topology, these networks are susceptible to security threats. Black hole attack is one of the route disruption attacks that cause a greater damage to the network. In this attack a malicious node belie that it is having shortest path and traps packets thereby degrading network performance. MANETs pose a greater challenge for routing protocols. In this paper AODV (Ad hoc On Demand Distance Vector Routing) protocol is used for route establishment since it is an efficient routing protocol but it lack with security issues. Hence well known cryptographic algorithm such as RSA Algorithm is used for providing a secure routing between mobile nodes even in presence of malicious nodes .In brief, this paper presents a counter measure to overcome black hole attack.

I. INTRODUCTION

Wireless Networks are gaining its popularity due to its ease of deployment, more economic and so on. These networks don't have any constraints of wired networks. Wireless networks can be categorized into infrastructure Wireless networks and infrastructure less wireless networks [1]. MANET (Mobile Ad hoc Network) is an infrastructure less wireless network where mobile nodes can move freely and can form network. Since these networks don't have infrastructure the communication occurs within the transmission range due to limited resource of energy for each node. Routing Protocols plays an important role in MANET for connectivity between nodes and can be classified into Proactive routing protocols, Reactive routing protocols and Hybrid routing protocols. Proactive routing protocols uses routing table and exchanges link information in between nodes whereas reactive protocol establishes routes only when nodes are ready to communicate means nodes does not exchange routing information. Hybrid combines the features of both proactive and reactive routing protocols. Due to the absence of centralized authority MANET is more susceptible to attacks by selfish nodes or malicious nodes. Although Routing protocols plays an important role for communication in MANET they run in un-trusted situations .One of the severe attack is Black Hole Attack. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to it [2].
A typical MANET architecture is as shown:

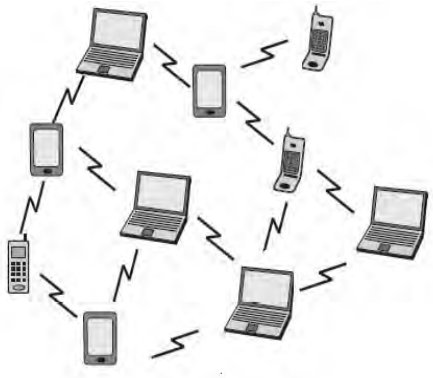

Figure 1: MANET Architecture

II. BACKGROUND

Before moving onto the Design and Implementation first we highlight the basic requirements of the system in a flow. First we describe the AODV protocol and its operation. Next routing attacks on MANETs are described.

Then Black hole attack and its effect on AODV described. In the Next Session Implementation Part will be explained.

2.1OVERVIEW OF AODV PROTOCOL

An AODV (Ad hoc on demand Distance Vector) protocol is an on demand routing protocol.

AODV is a collaborative protocol, allowing nodes to share information about each other[11]
The Ad-hoc on demand Distance Vector (AODV) algorithm enables dynamic, self starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network [3].This algorithm require some criteria to make routing decisions such as hop count, sequence number, latency, bandwidth etc.
AODV uses a broadcast route discovery mechanism as is also used with modifications in the Dynamic Source Routing (DSR) algorithm. The most distinguishable feature of AODV is it makes use of Destination Sequence number.
The combination of above techniques gives rise to AODV that uses bandwidth efficiently, data traffic is responsive to changes in topology and provides loop free routing.

2.1.1 AODV OPERATION:

AODV makes use of 3 control messages for route establishment namely RREQ (Route Request), RREP (Route Reply) and RERR (Route Error**)**

AODV operation occurs in two phases namely:
1) Route Discovery Phase and
2) Route Maintenance Phase.

1)Route Discovery Phase: The route Discovery process is initiated whenever a source node wants to transmit packet to destination first it checks link information in its table .Every node maintains two separate counters for a node sequence number and a broadcast ID. The Fields of RREQ is as shown below:

Source address	Source sequence number	Destination address	Broadcast ID	Hop Count

Source node broadcasts RREQ message to whole network. The range of dissemination of such RREQs is indicated by TTL or Hop count in the field, when hop count is a downward counter, means when hop count becomes zero then the packet is not forwarded further or in other way that packet is dropped [3]. If the destination is beyond the transmission range of source node then RREQ is rebroadcasted by the neighboring nodes which is having fresh enough and shortest route to destination. A Source Sequence number is used to avoid looping in the network. Once the destination receives RREQ message then it generates destination Sequence number and revert back to source by sending RREP message. RREP message is sent in a uni-cast way to source node [2]. The Fields of RREP is as shown:

Source address	Destination Address	Destination Sequence number	Hop Count	Lifetime

There may be some conditions like link failure which affects the network operation. To overcome this, AODV makes use of RERR (Route Error) message. When some link terminates or deactivates then all the nodes supposed to know about the link termination. So to tell the nodes about the link termination, RERRs are sent to every node in the ad hoc network so that every node can invalidate their route entries which are having routes through the terminated or deactivated link [3].

2) Route Maintenance Phase: Movement of nodes not participating in process does not affect the routing to destination path. If the source node moves during an active session, it can reinitiate the route establishment procedure. When either the destination or some intermediate node moves, a special RREP is sent to the affected source node.

Upon receiving notification of broken link, the source node can restart the route establishment procedure. To determine whether the route is still needed, a node may check whether the route has been used recently, as well as inspect upper level protocol to check whether connections remain open using the indicated destination. If the source node still requires the connection, it sends RREQ with a sequence number of one greater than previously known sequence number, to ensure that it builds a new valid route and that no nodes reply if they regard the previous route as valid. The below figure shows the AODV routing:

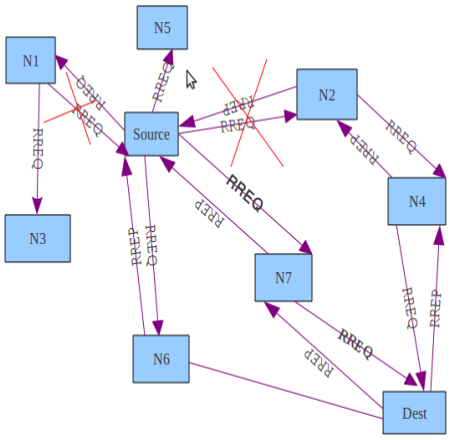

Figure 2: Routing in AODV

2.2 ROUTING ATTACKS IN MANETS:

Routing plays a very important role in MANETS. It can also be easily misused, leading to several types of attack. Routing protocols in general are more prone to attacks from malicious nodes. These protocols are usually not designed with security function and often are very vulnerable to node misbehavior. This is particularly true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process. Making routing protocols efficient often increases the security risk of the protocol and allows a single node to significantly impact the operation of the protocol because of the lack of protocol redundancy.

Examples of routing attack are as shown below:

Black Hole attack: In this attack[2] a malicious makes use of routing protocols to misrepresents that it is having the shortest and fresh enough route to destination without checking the availability of routes and drops the packets without forwarding further, thereby degrading network performance.

Wormhole Attack: In a wormhole attack [9], an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack: An attacker that performs a replay attack is retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes.

Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray-hole attack [8] has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain conditions.

Flooding attack: In flooding attack [10] multiple RREQ'S are sent from void IP addresses if the scope of the IP address is known else random IP addresses are chosen and the network is flooded with a large number of RREQ'S hence, the name flooding. When flooding attack takes place in a particular route the data packets discover the secure route and reach the destination.

2.3 BLACK HOLE ATTACK AND ITS EFFECT ON AODV:

Black hole attack is a route disruption attack [4] .This attack occurs during route discovery phase. In this attack a malicious node belie that it is having shortest path and traps packets thereby degrading network performance. When a malicious node starts trapping the packets black hole comes into picture. Black hole is also called packet drop attack as it keeps on drops the packets in Ad Hoc Networks [4].

When a source node desire to communicate with other node in a network, it initiates route discovery mechanism by broadcasting RREQ message to its neighboring nodes. Malicious node being a part of network sends back RREP soon after receiving RREQ there by misleading source that it is having the shortest path and fresh enough route. The source node responds to RREP sent by malicious node discarding RREP from other nodes as it reaches quickly. Then source node starts packet transmission to that malicious node. In this way black hole attack comes into picture.

In black hole attack hop count value is set to lowest value and the sequence number is set to the highest value. Malicious node send RREP to the nearest available node which belongs to the active route or it can also be sent directly to the source node if there is a route. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node [3]. The malicious node will drop all the data to which it belong in the route.. Therefore packets will not be forwarded to destination. Black Hole Attack is as shown below. [3].

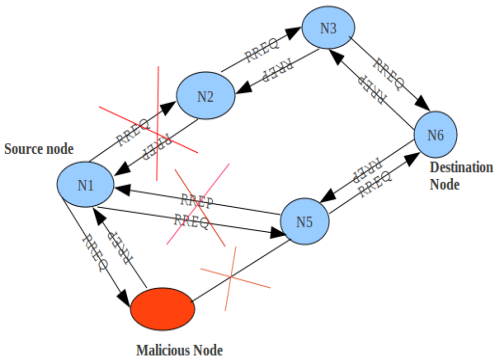

Figure 3: Black Hole Attack

In the above Figure N1 is source node and N6 is the destination node.N4 node is made malicious. It clearly explains Black hole attack.

2.4 CRYPTOGRAPHY:

Cryptography is the study of mathematical techniques concerned with protecting information or data from adversaries. Cryptography provides security of information such as Availability, Authenticity, data confidentiality, Data integrity and Non repudiation. Also it provides secure routing in MANETs.
Several Cryptographic primitives of functions have been designed in order to achieve the objectives. These primitives can be divided as:
1. Symmetric Key Cryptography: It involves the use of single key.
***2. Asymmetric Key cryptography*:** It involves the use of two keys
***3. Message digest*:** It does not involve use of any keys.

Conventional symmetric key cryptography makes use of one key that is shared by both sender and receiver. In this scheme distribution of key must be taken into consideration. Disclosure of this key will result in compromise of communication hence we make use of Asymmetric key cryptography or Public key cryptosystems.
Asymmetric key cryptography suits for providing security in MANETs since it makes use of 2 keys such as Public key and private key.
Public key defines encryption method while private key defines decryption method. Public key may be known anyone in the network while private key is supposed to be known only to one creating a message. These 2 keys are not same but related by mathematical values. Also it is infeasible to obtain private key knowing only public key and algorithm.
Public Key encryption does not require secure channel instead it requires authenticated channel for ensuring genuineness of the public key of other party. Some of the examples are RSA algorithm, ELGAMAL Algorithm and Rabin Algorithm.

RSA has several advantages such as ease of implementation, key size is smaller, problem solving, higher security and patent free since from 2000 etc.

III. IMPLEMENTATION DESIGN

In this paper, a cryptographic approach has been proposed for secure routing to overcome black hole attack in MANETs. In this approach hop count is encrypted using famous well known RSA (Rivest Shamir Adleman) algorithm.
Black hole attack occurs in route discovery phase. Basically black hole attack is modification of hop and immediate response using sequence number in the field of RREQ.
In this paper we considered a scenario of 6 nodes with 2 phases of execution: In first phase one of the nodes is made malicious by modifying AODV routing protocol and in second phase traffic is made flow even in presence of malicious node just by encoding hop count since destination can decrypt it using RSA algorithm.

3.1 RSA Algorithm

RSA algorithm is public key cryptographic algorithm that makes use of 2 keys namely public key and private key [5].
If RSA keys do not exist, they need to be generated. The key generation process is usually slow but it is performed seldom. It involves three steps: Key Generation, Encryption and Decryption [5].

Key Generation: Prime integers are used for key generation.

1. n =p*q
(n is used as modulus for both public key and private key)
2. Compute $\varphi(p*q) = (p-1)*(q-1)$.
3. Choose an integer e such that $1 < e < \varphi(p*q)$, and GCD of e and $\varphi(p*q)$ must be 1.
   - e is released as the public key exponent.
   - e having a short bit.
4. Determine **d** (using modular arithmetic) which satisfies congruence relation.
   d*e =1(mod($\varphi(p*q)$))

d is kept as the private key exponent

Encryption:
Destination node transmits its public key (n, ,e) to Source node and keeps the private key secret then source wants to send message **M** to Destination
It first turns **M** into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c corresponding to:

$$C \equiv m^e (mod\ n)$$

Decryption:
Destination node can recover m from c by using its private key exponent d by the following computation:

$$C^d \equiv m(mod\ n)$$

Given m, Destination can recover the original message **M** by reversing the padding scheme.

IV. SIMULATION RESULTS

We have simulated black hole attack on NS2 [6].

Packet Delivery Ratio: The ratio of data delivered to the destination to the data sent out by the source [7].

We created a scenario of six mobile nodes. In that one of the nodes is made malicious with simulation parameters such as PDR, node speed, time factor.

An output window under different time is shown below:

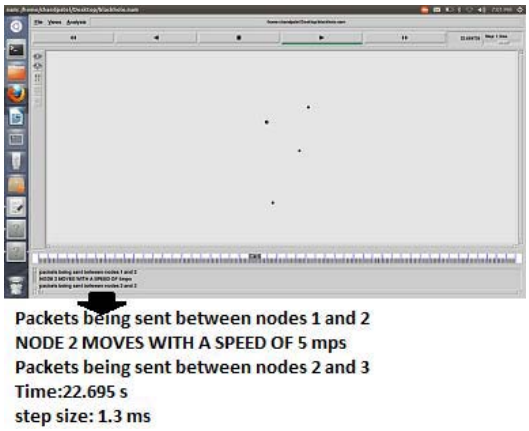

Figure 4: Output NAM window 1

Description: The above figure shows output NAM window which shows network operation at 22.695 second. NAM (Network Animator Window) is a pictorial representation of output. It is obtained by executing command nam blackhole.nam. (Given blackhole.tcl as name of TCL file) .In this scenario packets being sent between nodes 1 and 2,Node 2 moves with a speed of 5mps, Packets being sent between nodes 2 and 3.

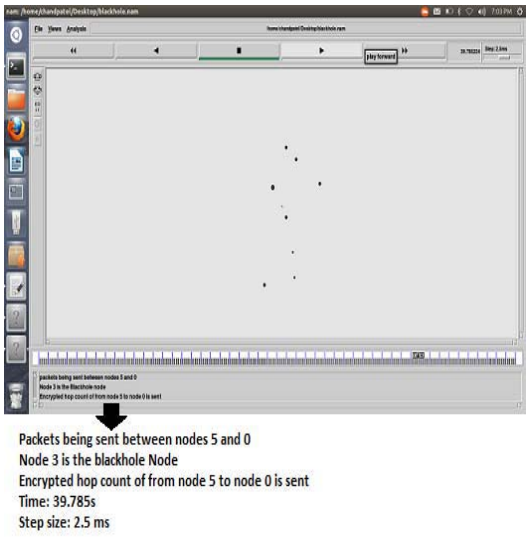

Figure 5: Output NAM Window 2

Description: Figure 5 shows output NAM window which shows network operation at 39.785 seconds. NAM (Network Animator Window) is a pictorial representation of output. It is obtained by executing command nam blackhole.nam. (Given blackhole.tcl as name of TCL file) .In this scenario packet being sent between nodes 5 and 0, here Node 3 is made malicious, and hop count is encrypted. Hence performance will be same even in presence of Black hole node since it is detected and traffic is deviated towards destination.

V. CONCLUSION

Security of MANETs can be achieved using two approaches such as secure routing and intrusion detection system. In this thesis, a cryptographic approach such as RSA algorithm is used for secure routing. Here malicious nodes can be detected since hop count field and sequence numbers are encrypted. Hence Latest sequence number packets are received by destination node thereby decreasing memory overhead and to make network loop free. Finally the paper explained the counter measures for Black hole attack. This mechanism must be tested for larger networks can be considered as future work.

REFERENCES

[1] Mohit Kumar, Rashmi Mishra "*An Overview of MANET: History, Challenges and Applications"* Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3 No. 1 Feb-Mar 2012.

[2] H. A. Esmaili, M. R. Khalili Shoja , Hossein gharaee "*Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator*" , World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 2, 49-52, 2011

[3] Rajkumar Singh, "*Ad-hoc On-Demand Distance Vector Protocol and Black Hole Attack in AODV*" CS 399: Seminar, Term Paper, 10thApril 2012.

[4] Rakesh kumar Sahu,Narendra S chaudhari "*performance evaluation of ad hoc network under black hole attack* 978-1-4673-4805-8/$31.00, IEEE 2012

[5] Prasad lokulwar* and vivek shelkhe, "*Security aware routing protocol for MANET using asymmetric cryptography using RSA algorithm",* BIO-INFO Security Informatics ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, pp.-11-14. 2012.

[6] Kameswari Chebrolu *"NS2 Tutorial"* Dept. of Computer Science and Engineering, IIT Bombay

[7] M. Khalili shoja*, H. Taheri*, and S. Vakilinia**,"*Preventing Black Hole Attack in AODV through Use of Hash Chain"* *Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran

[8] Megha Arya, Yogendra Kumar Jain "*Grayhole Attack and Prevention in Mobile Adhoc Network"* International Journal of Computer Applications (0975 – 8887), Volume 27– No.10, August 2011

[9] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah *"MANET Routing Protocols and Wormhole Attack against AODV"*IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[10] S.Kannan, T. Kalaikumaran, . S.Karthik, V.P. Arunachalam "*A Review on Attack Prevention methods in MANET"Journal of modern mathematics and statistics"* 5(1) :37-42, 2011, ISSN 1994-5388, Medwell journals, 2011

[11] Ochola EO, Eloff MM "*A Review of Black Hole Attack on AODV Routing in MANET"*