Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/100228, December 2016 ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection and Prevention of Black Hole Attack using Rivest Cipher 6 Algorithm

Satish Kumar*, Mrigana Walia, Chitranjan Tanwar

University Institute of Information Technology, Himachal Pradesh University, Gyan-Path,
Summer-Hill, Shimla - 171005, Himachal Pradesh, India;
satish.shimla89@gmail.com, mrigana9@gmail.com, chitu_319@yahoo.com

Abstract

Wireless ad hoc network is oneself configuring network that is used to establish network between nodes spontaneously. The impregnable and minimal pathway between informant/source and destination provide the reliable data transmission. We use MAODV protocol. In MAODV protocol we use Genetic Algorithm to make it more reliable for routing. It is the receptive routing protocol which used to build the minimal path by comparing hop counts RivestCipher-6 is the algorithm which is used to procure data using stream cipher text to be sent towards destination. Here, we give the noble approach to prevent black hole attack.

Keywords: Black Hole, Genetic Algorithm, MAODV, Rivest Cipher6

1. Introduction

Wireless ad-hoc network is the gathering of "peer" portable node that are equipped for communication with each other without help centralized system. There is no immobile base station for correspondence. Every node itself goes about as route for sending and accepting data packets to/from other node in network, node in the network dynamically set up routing process by themselves. There is likelihood of more security dangers in the event of portable and specially ad-hoc network[1] as contrast with unify wireless network. ad-hoc network is self-arranging framework small network of terminal devices connected by each other to wireless. every node in ad-hoc network is freely move any directional, and it will be subsequently swerve its connections to different device regularly. Each must forward activity inconsequential its own utilization, the elemental challenge in edifice a MANET is preparing every node persistently keep up data required to appropriately course activity. Mobile Ad hoc Network is an accumulation of free portable node that convey to each other through radio waves. Mobile node that in radio scope of each other can straightforwardly convey, while others require the intermediate node to travel the packet. These systems are completely circulated, and work wherever without assistance of any foundation. This property form these systems exceedingly adaptable and powerful. The MAODV[2] is the receptive routing protocol which frame up minimal path between the starting and destination for information transmission but the performance is affected when the node fails the discovery of route has to be so to improve the trust and stability in routes we use on demand routing protocol thus SBMR discover multiple route in between source and destination order to say a backup route for the destination node in case of failure of link which avoid reroute discovery of destination and to find the shortest path from multiple path we use genetic algorithm in our protocol.

*Author for correspondence

Introduction of Black Hole Attack

Black hole attack is one of the most possible attack in MANET. In which black node advertise itself for having the minuscule path to the end node and source node think that it's a genuine node and send the data to black node result black node will dropped whole data shown in Figure the source node is 0 transmit a route dicover request message to discover a route for sending packet destination node 2 route request (RREQ) transmit by node 0 is incur by nearest nodes 1, 3 and 4. Node 4 send a path reply message instantly without even out having a path to receiver node 2. Route reply message from a malicious node is the first to come at an informant node because it is the intruder node now a source node updates its routing table for the new route to the particular node and rejects any RREP message from other nearest nodes even from an original node. Once a source node saves a route, it starts sending data packets to a malicious node hoping they will be forwarded to a destination node. Malicious node (performing a black hole attack) drops all data packets rather than forwarding them onto destination.

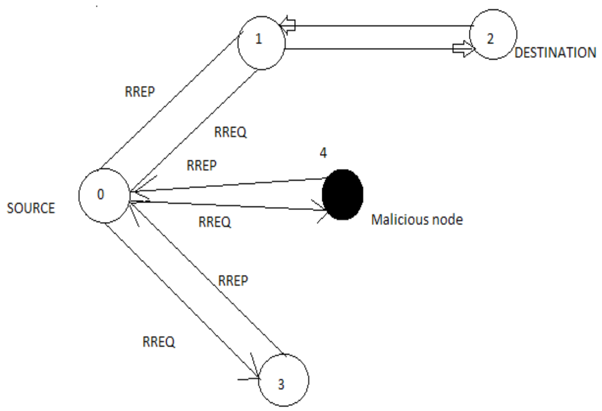


Figure 1. Black Hole Attack.

Routing Protocol

Routing protocol is the protocol that state the how the router communication with each other. It is a set of rules used by routers to find the most suitable paths into which they should forward packets towards their intended

A) Proactive Routing Protocol: In this kind of routing protocol, each node in a system or network maintains one or more routing tables which are over hauled routinely with in time. Each node broadcast message to the entire network if there is a change in the network or system topology. However, it will bring extra overhead cost due to the maintaining up-to-date data and as a consequence; throughput of the network may can also affected but it provides the real information to the availability of the network. The example is Distance vector protocol, Destination Sequenced Distance Vector (DSDV) protocol, Wireless WSR, Fisheye State Routing (FSR) protocol are the examples of on demand protocol.

B) Reactive Routing Protocol: In this kind of protocol, every vehicle in the system finds or keeps up a course taking into account request. It surges the control message by worldwide telecast amid finding a course and when course is found then transfer speed is utilized for information transmission. The fundamental point of interest of this convention is needs less routing data however the hindrances are that it creates huge control bundles because of course distinguishing proof amid topology changes which happens much of the time in MANETs and it cause acquires higher inertness. The illustrations are these sorts of convention are Dynamic Source Routing (DSR), Associatively Based Routing (ABR) conventions and AODV.

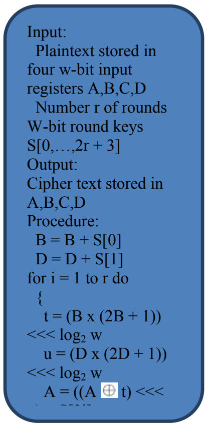
C) Hybrid Protocols: It is a Mixture of proactive and reactive protocols taking the best feature from both types Protocol.

RC6 RIVEST CIPHER

RC6 (Rivest cipher 6) it is a symmetric key square cipher produced from RC5. It was create by Ron Rivest, Ray Sidney to meet the fundamental necessities of the Advanced Encryption Standard (AES). RC6 proper have a block size of 128 bits and compatible with key sizes of 128, 192, and 256 bits, as was in RC5, it may be characterized to assist a vast variety of word-length, key size, and number of rounds. RC6 has similarity with RC5 in XOR operations, data-dependent rotations and modular addition. RC6 uses two parallel RC5 encryption process and used an extra multiplication in order to make the rotation reliant on every bit in a word, and not like least significant bits.

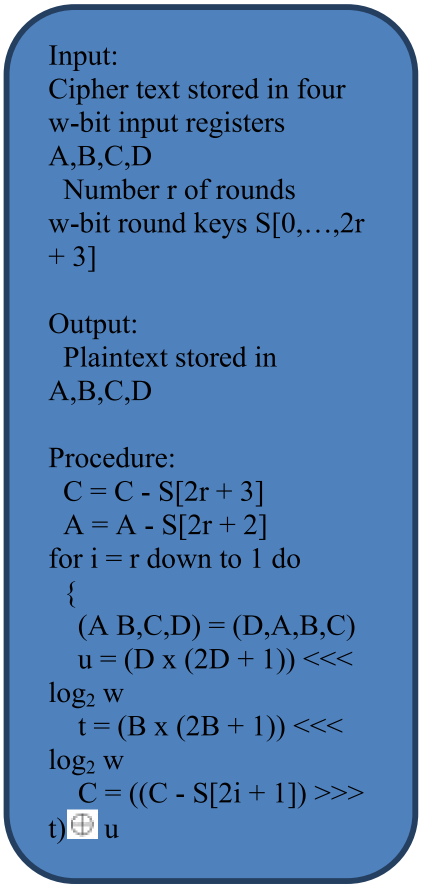
Encryption and Decryption with RC6

The procedures of encryption and decoding are both made out of three phases: pre-brightening, an inward circle of rounds, and post-brightening. Pre-brightening and post-brightening evacuate the likelihood of the plaintext uncovering part of the contribution to the first round of encryption and the figure content uncovering part of the contribution to the last round of encryption). The square encryption handle showed in Figure 1 utilizes operations as a part of Figure 4 beneath. To begin with, the registers B and D experience pre-brightening. Next, there are r rounds, which are assigned by the "for" circle. The registers B and D are put through the quadratic condition and turned (log2 w) bits to one side, individually. The subsequent estimation of B has an elite or (XOR) operation with An, and D with C individually. This esteem t is then left-turned u bits and added to round key S[2i]; the subsequent estimation of D and C is left-pivoted t bits and added to round key S[2i + 1]. In the last phase of the round, the enroll qualities are permuted, utilizing parallel task, to blend the AB calculation with the CD calculation, expanding cryptanalytic many-sided quality. Finally, registers An and C experience post-brightening. In spite of the fact that encryption and decoding are comparative in general structure, the nitty gritty contrasts bear exchange. For RC6 decoding, the system starts with a pre-brightening venture for C and A. The circle keeps running backward for the quantity of r rounds. Inside the circle, the primary undertaking is parallel task. From that point, the previously mentioned quadratic condition is utilized on D and B individually. The subsequent esteem for u, and t individually, is left-turned (log2 w) bits. The round key S[2i + 1] is subtracted from enroll C esteem, the consequence of which is correct pivoted t bits; round key S[2i] is subtracted from enlist An esteem, the after effect of which is correct turned u bits. This subsequent esteem including register C has an elite or operation with u, A with t individually. Subsequent to finishing the circle, D and B.



```
Input:
  Plaintext stored in
four w-bit input
registers A,B,C,D
  Number r of rounds
W-bit round keys
S[0,…,2r + 3]
Output:
Cipher text stored in
A,B,C,D
Procedure:
  B = B + S[0]
  D = D + S[1]
for i = 1 to r do
   {
    t = (B x (2B + 1))
<<< $\log_2$ w
    u = (D x (2D + 1))
<<< $\log_2$ w
    A = ((A ⊕ t) <<<
```

Figure 2. RC6 Encryption with RC6-w/r/b.



```
Input:
Cipher text stored in four
w-bit input registers
A,B,C,D
  Number r of rounds
w-bit round keys S[0,…,2r
+ 3]

Output:
  Plaintext stored in
A,B,C,D

Procedure:
  C = C - S[2r + 3]
  A = A - S[2r + 2]
for i = r down to 1 do
   {
    (A B,C,D) = (D,A,B,C)
    u = (D x (2D + 1)) <<<
$\log_2$ w
    t = (B x (2B + 1)) <<<
$\log_2$ w
    C = ((C - S[2i + 1]) >>>
t)⊕ u
```

Figure 3. RC6 Decryption with RC6-w/r/b.

Operation	Description
a + b	Integer addition modulo 2^w
a – b	Integer subtraction modulo 2^w
a ⊕ b	Bitwise exclusive-or (XOR) of w-bit words
a x b	Integer multiplication modulo 2^w
a <<< b	Rotate the w-bit word a to the left by the amount given by the least significant ($\log_2$ w) bits of b
a >>> b	Rotate the w-bit word a to the right by the amount given by the least significant ($\log_2$ w) bits of b
Enc: (A,B,C,D) = (B,C,D,A) Dec: (A,B,C,D) = (D,A,B,C)	Parallel assignment of values on the right to registers on the left.

Figure 4. Algorithmic operation Table.

2. Proposed Scheme

The Black hole attack is conceivable in the MANET. There are so many techniques or protocols that are used to detect or prevent this kind of attack. Now we projected a noble technique to be prevent the black hole attack that is more efficient of other technique. In proposed scheme we use the MAODV protocol in this protocol we modified the AODV protocol. In MAODV we add the feature of genetic algorithm[3] that is for the route set or beneficial in that case when the link faces failure it also backup the route. Every node maintains the table based on several parameters such as source and destination IP address, Port number, duration of connection, protocol used which is beneficial for identification of malicious nodes. And also we use the rivest cipher 6 algorithm, for a secure channel to be established betwixt the sender the receiver before the data transmission. For securing and preventing the data from malicious nodes we use Rivest Cipher 6.

3. Future Work and Conclusion

Black hole attack is primary security threat. Its sleuthing is the main matter of concern. Many of the researchers have directed many noble techniques to propose prevention mechanisms for black hole problem. There are different security mechanisms are introduced to prevent black hole attack. We also propose the most efficient approach to preclude the attacks. That will be dissimilar from the previous given technique In our Further work, we will be implement this given intrigue in the network simulator NS3 and compare the results with different parameter of the existing schemes, so use the different technique to detect and Black hole attack.

4. References

1. Kavi Joshi. Three Way Techniques for Preventing Black Hole Attack in MANET Using AODV Protocol. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization). 2016 February; 4(2).
2. Anjali P Rathod. Detection Mechanism for Black hole attacks in MANET. International Journal of Advanced Research in Computer and Communication Engineering. 2016 April; 5(4).
3. Christeena Joseph. Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios. International Journal of Advanced Research in Computer and Communication Engineering. 2015 November; 8(29).