# WORMHOLE ATTACK DETECTION USING RC4-STREAM CIPHER ALGORITHM IN MANET

**[1]Rajkumar M.,[2] Karthika J**

[1] Department of Information Technology, [2] Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore , Tamilnadu, India.

***Abstract***

The wireless network is prone to many attacks. This paper focuses on wormhole attacks. A novel algorithm is proposed which uses connectivity information to identify the wormhole attacks. The proposed work does not use any special hardware object or location information. The novel algorithm is completely limited locally by making the technique widely applicable. The algorithm does not depend on wireless communication models. But, model knowledge and distribution of the node helps to build the RC4 algorithm. Even for very low density networks where probability of disconnection is very high, the discovery prospect remains very high. To enhance the security of the internet Network RC4 algorithm is used. The RC4 algorithm has two stages. The two stages are PRGA and KSA. RC4 steam cipher algorithm is implemented on java and it offers the fast encryption and decryption, low down the resources utilization, low time and space complexity as compare to other different algorithms.

Keywords: **wormhole attack, secure routing, connectivity information, RC4 algorithm.**

## 1. INTRODUCTION

Wireless ad hoc and sensor networks are typically used out in an open, uncontrolled environment, often in hostile territories. Some important applications for such networks come from military and defence arenas. Use of wireless medium and intrinsic collaborative nature of the network protocols make such network vulnerable to various forms of attacks. In this paper our focus is on a particularly overwhelming form of attack, called *wormhole* attack [1]–[3].Here, the adversary connects two distant points in the network using a direct low-latency link called the *wormhole link*.

The Wormhole link can be established by using a network cable and any form of "wired" link technology or a long-range wireless transmission in a different band. The end-points of this link (*wormhole nodes*) are equipped with radio transceivers compatible with the adhoc or sensor network to be attacked. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

A wormhole attack is a particularly severe attack on MANET routing, where two attackers connected by a high-speed off-channel link, are strategically placed at different ends of a network. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them.

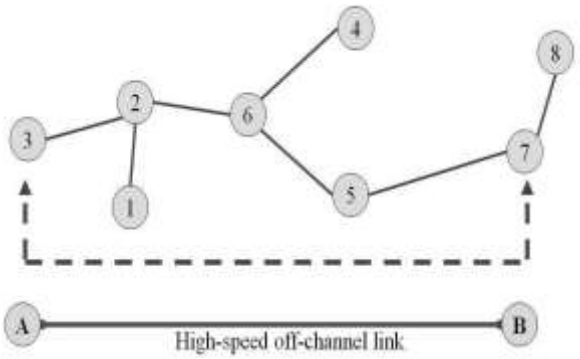


**Fig.1 Wormhole attack**

In Fig.1, when node 3 sends a HELLO message, intruder A forwards it to the other end of the network, and node 7 hears this HELLO message. Since 7 can hear a HELLO message from 3, it assumes itself and node 3 to be direct neighbors. Thus, if 7 wants to forward anything to 3, it will do so through the wormhole link, effectively giving the wormhole attackers full control of the communication link.

In the above Figure, if 3 wants to communicate with 7, it sends out a request, which a wormhole, once again forwards without change to the other end of the network, - directly to node 7. A request also travels along the network in a proper way, so 7 is lead to believe it has two possible routes to node 3: a 4-hop route through nodes 2, 6, and 5, and a single-hop direct link. Protocols will then select the shortest route, once again giving wormhole attackers full control of the link.

Majority of adhoc routing protocols rely on the correctness of their neighbors information for routing decisions, thus allowing wormhole-induced disruptions to have greater effects. For example, in the situation described in Figure, where nodes 3 and 7 think they are direct neighbors, nodes 5 and 8 will then think they are two hops away from node 3 (going through node 7), and will communicate with node 3 through the wormhole link as well.

In this paper, for detecting wormhole attacks we extend an algorithm that is purely based on local connectivity information. Such information is often collected any way by various upper layer protocols such as routing, thus may not present any additional overhead. No additional hardware object is needed making the approach universally applicable. No timing analysis is done ensuring that we can detect even physical layer attacks. Our technique does not use location information and is able to detect attacks that are launched even before the network is set up, that may influence localization. We focus on the following steps in our work.

1. Initially the topology is constructed based on node information.
2. After the topology is created, the nodes are connected using the given connectivity model.
3. Once the connectivity graph is established, the following experiments are performed:
   a) Connectivity in the entire networkis checked. The network is assumed disconnected if any two nodes do not have a path to each other.

b) The wormhole detection algorithm is run to see whether there is a false positive. (At this time, there is no 1While our technique is independent of whether the entire network is connected or not, connected networks are more useful from a practical standpoint)
c) A wormhole attack is established between two randomly chosen locations. The algorithm is run again to see whether it detects the wormhole.

## 2. RELATED WORK

Numerous physical approaches have been proposed to secure the neighbour discovery process. Most of the solutions presented so far require that the nodes handle information about self-location, perform clocks synchronization or rely on specialized antennas or on information such as trust relationship. Only few solutions have been proposed to secure the overall end-to-end route discovery process. Other approach contains timing and/or position information to packets. This restricts the maximum transmission distance permitted to a packet. They propose two kinds: geographical and temporal. To use geographical approach, each node must know its own location and all nodes must have loosely synchronized clocks. To use temporal approach, all nodes must have tightly synchronized clocks. Thus, if a receiving node determines that the neighbor discovery signal of a given node has traveled too far, the node should discard it.

Another approach is to estimate the distance separating two nodes from the round-trip travel time taken by a message and its acknowledgement. This mechanism relies on a specialized hardware allowing the destination to send a response to a one bit challenge message as fast as possible. Several approaches have been developed to prevent or to detect wormhole attacks. The first three solutions address mainly the closed wormhole attacks. They present how to protect the neighbour discovery process. Hu *et al.* [4] propose the addition of *leashes* containing timing and/or position information to packets. A leash restricts the maximum transmission distance permitted to a packet. They propose two kinds of leashes: geographical and temporal. To use geographical leashes, each node must know its own location (e.g. GPS) and all nodes must have loosely synchronized clocks. To use temporal leashes, all nodes must have tightly synchronized clocks. Thus, if a receiving node determines that the neighbour discovery beacon of a given node has travelled too far, the node should discard it.

C˘ apkun *et al.* [5] estimates the distance separating two nodes from the round-trip travel time taken by a message and its acknowledgement. This mechanism relies on a specialized hardware allowing the destination to send a response to a one bit challenge message as fast as possible. Hu and Evans [6] use directional antennas to detect wormhole attacks. If a node uses a specific sector to communicate with a neighbour, this neighbour should use its opposite sector. The existence of a wormhole would introduce inconsistencies in the network that could be detected by the other nodes simply by adding some sector information to the packets. Finally, Qian *et al.* [9] present a different approach to detect wormhole attacks. The solution is based on statistical analysis of the information gathered during the multipath routing process (SMR). A link generating a wormhole attack should be used by the routing protocol with an unusually high frequency.

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. The demand on available bandwidth is significantly less than other proactive protocols as AODV doesn‟t require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path.

## 3. WORMHOLE DETECTION ALGORITHM

### 3.1 RC4 Algorithm

To improve the security of the internet Network and for internet applications like: E-Commerce Application RC4 algorithm is used. The RC4 stream cipher algorithm is most used algorithm to provide the confidentiality over the different networks like: Sensor, wireless, Internet, Mobile and so on. The RC4 algorithm is two stages algorithm. The two stages are PRGA and KSA. Vulnerabilities are found in both the stages. RC4 steam cipher algorithm is providing the fast encryption and decryption, low resources utilization, easy to understand and implement, low time and space complexity as compare to other different algorithms.

### 3.2 RC4 Stream Cipher Algorithm

RC4 algorithm was introduced by the Rivest in [years].This is the Symmetric stream cipher Algorithm. This is the most used algorithm. RC4 steam cipher algorithm is providing the fast encryption and decryption, low resources utilization, easy to understand and implement,low time and space complexity as compare to other different algorithms. The algorithm is dividing into two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm). KSA as the first stage of algorithm also known as initialization of S (s is state vector ) and PRGA known as stream generation in the RC4.In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table,the key stream is generated that is XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage following steps are done.

1. Inputting the variable length key of size from 1 to 256
2. Initialize the key matrix as per the size of the input key
3. Initialize the State table of fixed size 256 bytes from the value 0 to 255 in ascending order.

4. Using the key matrix of variable size done the permutation on the S table.
5. Output of the KDA, the final prepare S table after shuffling operation.

In this manner the KDA generate the State Table (State Matrix) of 256 bytes.

***Algorithm:***

N=256
Shuffle function using for Swapping

***KSA:***

**1.** Inputting two Keys (k1 & k2) (Key Lengths)(base keys)
**2.** initialize the two Key[length] //
generate on the bases of two sub keys
For i=0 to k1
Random1[i]=random value;// (secret random1)
End for
For i=0 to k2
Random2 [i] =random value ;//( secret random2)
End for
**3.** Initialize the Two Temporary Matrix and State Matrix
For i=0 to N
Random_temp1[i]= value
Random_temp2[i]= value
STATE1[i]=i;
STATE2[i]=i;
End for
**4.** Permutation on State Matrix
j1=j2=j3=0
For i=0 to N
**J1=(j1+state1[i]+state1[j1]+random_temp2[i]+random_temp2[j1]+random_temp2[j2])%N;**
**J2=(j2+state2[i]+state2[j2]+random_temp1[i]+random_temp1[j1]+random_temp1[j2])%N;**
**shuffle(state1[i],state1[j1])**
**shuffle(state2[i],state2[j2])**
End for

***PRGA:***

**5.** Generate the random values used for encryption
i=j1=j2=0
while(True)
i=i+1 % N
**j1=j1+state1[i]+state2[j1]+state2[j2] % N**

**j2=j2+state2[i]+state1[j1]+state1[j2] % N**
shuffle(state1[i],state1[j1])
shuffle(state2[i],state2[j2])
indx1=(state1[i]+state1[j1]) % N
indx2=(state2[i]+state2[j2]) % N
byte1= state1[indx1]
byte2= state2[indx2]
CT= PT1 XOR byte1
CT1= CT XOR byte2
**Shuffle(state1[state2[i]],state1[state2[j1]])**
**Shuffle(state2[state1[i]],state2[state1[j2]])**
Wend( End While)

### 3.3 Encryption/Decryption Process

Data processes two times during encryption and decryption. But in this algorithm, the encryption and decryption has done on the bases of two key2. Let's understand through diagram

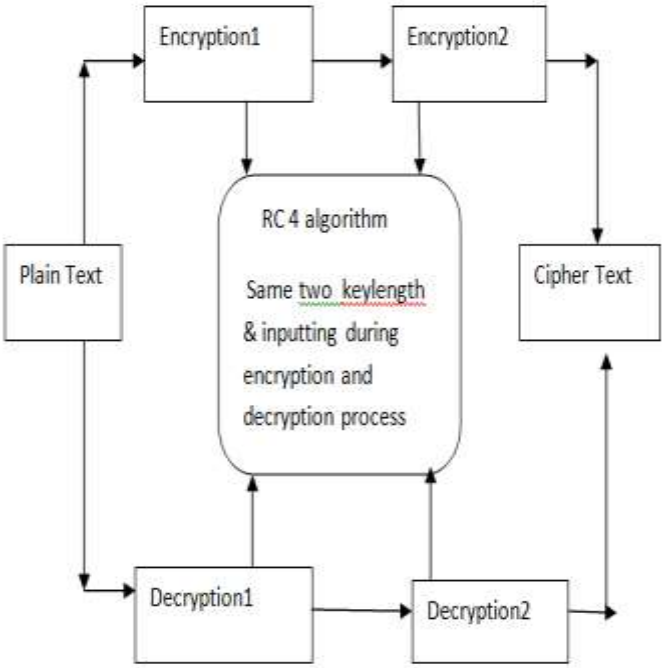


**Figure 2: RC4 Encryption and Decryption Process**

In figure2, the encryption and decryption process of PC2-RC4 algorithm is shown. In this algorithm, two different keylen1 and keylen2 as base key inputs, on the bases encryption does in two stages.

## 4. IMPLEMENTATION

### 4.1 RC4 Algorithm Output

```
inputting two keys:  100 100
Plaintext is =pardeeppushpendrapramodkumarji
Ciphertext is =?gØ□¾q5⁹⃣)Rë"j8RÛêç?ª□□Ôd □;?9
nano time 206058

Plaintext is =pardeeppushpendrapramodkumarji
```

### 4.2 RC4 algorithm

Keylen1=keylen2=100

| Data Size | Encryption Time |
|---|---|
| 100 | 281360 |
| 200 | 453344 |
| 300 | 577590 |
| 400 | 686855 |
| 500 | 905750 |

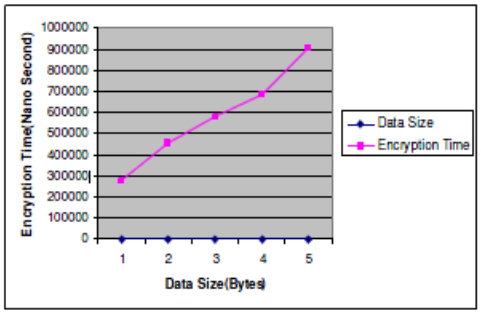


**Fig.3 RC4 Encryption Algorithms**

## 5. CONCLUSION

In this paper we propose a practical algorithm for wormhole detection. The algorithm is simple, localized, and is universal to node distributions and communication models.The proposed approach is implemented in Java and J2ME technology on a Pentium-III PC with 20 GB hard-disk and 256 MB RAM. The propose approach's concepts show efficient results of retrieving data from mobile nodes and has been efficiently tested on different systems.Thus this approach is very effective in detecting wormhole attack detection based on the connectivity information.

## REFERENCES

[1] ZhiguoWan ,Kui Ren ; Ming Gu "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", *IEEE Transactions On Wireless Communications*, vol. 11, no. 5, May 2017.

[2] F.Nait-Abdesselam,B.Bensaou,and T. Taleb, ―Detecting and avoiding Wormhole attacks in Wireless Ad-hoc Networks‖, in IEEE Communication Magazine.vol.46,April 2018,pp.127-133.

[3] G. Lee, D. k. Kim, J. Seo, ―An Approach to Mitigate Wormhole Attack in Wireless Adhoc Networks," IEEE International Conference on Information Security and Assurance, pp. 220-225, 2018.

[4] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Adhoc Networks, in Proc. of INFOCOM 2003, San Francisco, CA, USA, April 2013.

[5] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications,* vol. 24, pp. 370 – 380, 2016

[6] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proc. of the Network and Distributed System Security Symposium, 2014.

[7] Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity In-formation", Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA

[8] C.E perkins ,E.M Royer and SR Das." Ad-hoc on demand distance vector routing", the *2nd IEEE workshop on mobile com-puting system and application* pages 90-100, Feb. 2004.

[9] N. Song, L. Qian,X. Li. "Wormhole Attacks Detection in Wire-less Ad Hoc Networks: A Statistical Analysis Approach". *In Proceedings of the 19th IEEE International Parallel and Distrib-uted Processing Symposium,* pp. 8-15, 2015.

[10] Pardeep, Pushpendra Kumar Pateriya, " PC1-RC4 and PC2-RC4 Algorithms: Pragmatic Enrichment Algorithms to Enhance RC4 Stream Cipher Algorithm", *International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 3, June 2019.*