Detection of Black Hole Attack Using Random Code Division Method

J. Muthusundharam[1]
ME Scholar,
Department of Computer Science and Engineering,
Coimbatore Institute of Technology,
Coimbatore, India,

A. Priyadharshini[2],
Assistant Professor,
Department of Computer Science and Engineering,
Coimbatore Institute of Technology,
Coimbatore, India,

***Abstract*:- A mobile Adhoc network (MANET) is a collection of autonomous nodes to form a network without use of any supporting infrastructure. The network topology is unstructured and nodes may enter or leave at their will. A node can communicate to other nodes which are within its transmission range .So any node can act as a host or the router in the network, which results in security issues in MANETs. A prominent attack in MANETs is a Black hole attack. In this paper, we present a efficient method called Random Code Division Method (RCDM) for security in order to detect and prevent Black hole attack in MANETs. Black hole node is a malicious node which can mislead a normal node to forward the data through it and corrupt the data so that it can degrade the performance of the network. We validate our approach using network simulator.**

Keywords: MANET, Black hole, Authentication.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes to form a network without use of any supporting infrastructure. If the two communicating nodes are within the same sensing range they can communicate to each other individually, otherwise they can communicate through multi hops where nodes act as intermediate routers. In this type of network, nodes can enter in the network or leave the network at any time without informing to others. In MANETs, there is no guarantee that a path from source to destination is free from malicious nodes. Due to lack of central coordination, there are several attacks in MANETs. Active attack may harm or alter the data being transmitted across the network [4]. In the Sybil attack [5], a well known attack is a Black hole attack, which is created by a malicious node by sending a very quick reply with highest destination sequence number and shortest path. Black hole node can easily corrupt the information. To avoid such type of attacks, research community pays much attention towards the security of MANETs. The Black hole attack is addressed in the literature either by considering the energies of the nodes [8]. The first approach does not provide an effective solution to the Black Hole attack as the malicious nodes can be available in the network with different energies. In the second approach, providing certifications to the nodes that are mobile is difficult.

In this paper, we propose a effective method of security called Random Code Division Method (RCDM). For this purpose, we consider an additional field of one byte with the packet header to represent the code of source node. In our approach, the starting code of source node is '0' (i.e. 0000). In the first hop, a decimal number '01' (i.e. 0001) is added to the source code word. In the next hop, '02' (i.e. 0010) is added to the first hop code word and this process continues till destination node.

The rest of the paper is organized as follows. Section 2 presents the related work. In section 3, we describe our proposed approach. Section 4 presents the simulation results. We conclude the paper in section 5.

II. RELATED WORK

However, this scheme is having a poor response when collision occurs in the route where data packets are transmitted. Also this approach is imperfect due to less transmission power. Hu et al [5] presented a secure on demand routing protocol that deals with the life time and the control messages. However, this scheme does not have any authentication for the intermediate nodes. So, malicious node can easily enter in the network and can take part in the route and creates interference in the routing process.

Sharma et al [4] described a solution to the Black hole attack by setting the waiting time of the source node to receive the repeat request from other nodes. The authors assume that the waiting time is exactly equal to half of the route reply (RREP). However, this may not be true for multi hop network when the two routes from source to destination have enough time difference to receive request. Deng et al [3] presented a routing protocol in which every intermediate node requires to send a reply request message to the source node. However, this approach increases the routing overhead and also increases the delay from source to destination. Chandrakant [2] described an approach for protection to MANETs based on energy consumption of a node.

Lu et al [7] proposed a Secure Ad-hoc on-demand Distance Vector (SAODV) routing protocol to prevent Black hole attack in MANETs. This approach addresses only few of the security weaknesses of AODV, and thus Black hole attack cannot be removed completely. Deswal and Sing [4] proposed an enhanced version of SAODV protocol by giving password to each of the routing node. This approach may not

be valid when new nodes enter in the network, which degrades the performance of the network. In this paper, we propose a model that improves the performance of the network by giving the security at every hop based on the source code.

III. PROPOSED MODEL

In this section, we present our proposed method to find the Black hole attack in MANETs. We assume that all the nodes in the network have the same behavior, so that all nodes know the hop operation, we consider an additional field of one byte with the packet header to represent the code of source node and hop count. When the source node is ready to communicate with destination node through intermediate nodes, it appends an 4 bit data '0000' in the packet header to indicate the starting code and hop count. Then, the source node sends the data along with this code word to all its neighbors. All neighbor nodes will receive the data, however only those nodes can access it which knows the one hop operation (i.e., how to operate the code at one hop). In this way, Black hole attack can easily be detected and data can be protected from such attacks. At the next hop, a decimal number '01' (i.e. 0001) is added to the source code word. Similarly, '02' (i.e. 0010) is

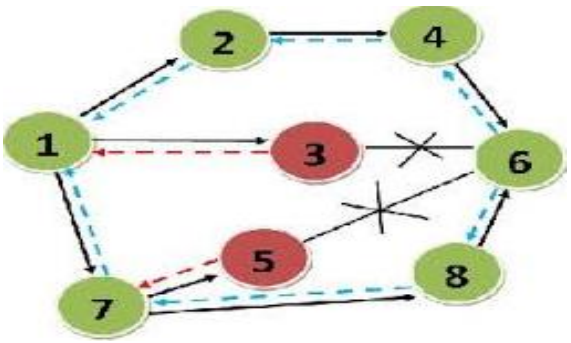

Fig. 1. Three hop MANET with Two Malicious Node

added to the next hop code word. This process continues till it reaches the destination. This approach is used to reduce packet loss.

Figure 1 shows the operation of three hop MANETs. In the figure, **3 & 4** represents Black Hole (Malicious Node), **1** represents source node, **2, 4, 6, 7** represent intermediate nodes and **6** represents destination node. Source node sends the route request to all its neighbors. only node 2 and node 7 can process the data by adding the one hop code word with the source node code word (see Table 1). Malicious node 3 and 5 cannot process it because it cannot understand the one hop operation. So Black hole attack can be easily detected.

In the next hop, node 2 and node 7 will forward the data along with one hop code to nodes 4, and 8. Again node 3 cannot access the data because it does not operate the code word as per the second hop operation. So nodes 3 and 4 can only access the data and process it towards the next node. This process continues till the data reaches the destination. Suppose any malicious node manages to know the hop count, still it cannot construct the code word at that hop stage as it does not know the operation of code word at that stage of hop count. So malicious node can be easily detected and thus it will not drop the packets.

Let the source code be represented by 1.

$S = 0000$

$Hop_1 = 0001$

$Hop_2 = 0010$

$Hop_3 = 0011$.

Table 1. Code word of 5-hops

S. No	Code Number	Hop Number
01	0000	O (Source node)
02	0000+0001=0001	Hop 1
03	0001+0010=0011	Hop 2
04	0011+0011=0110	Hop 3
05	0110+0100=1010	Hop 4
06	1010+0101=1111	Hop 5

Detection of Black Hole Attack Using Random Code Division Method

The complete code word for the individual hop can be represented as

Source code word = Source

= Source + Hop_1 =

First hop code word Hop_{CW1}

where Hop_{CW1} is the hop code at first hop and is equal to *Source* + Hop_1.

Second hop code word $= Hop_{CW1} + Hop_2 = Hop_{CW2}$

where Hop_{CW2} is the hop code at second hop and is equal to $Hop_{CW1} + Hop_2$. Similarly, the 'N^{th}' hop code ,

$Hop_{CWN} = Hop_{CW(N-1)} + Hop_N$

where Hop_{CWN} is the hop code at N^{th} hop and Hop_N is the N^{th} hop code. So the code word at any hop can be calculated as,

IV SIMULATION RESULTS

In this section, we describe the results of our approach and compare with the two existing approaches: Ad-hoc on-demand Distance Vector (AODV) and DSR[1] approach by using NS-2 Simulator. Figure 2 shows the variation of Packet Delivery Ratio (PDR) versus the simulation time of the source- destination pair. It can be observed that if the source-destination pair is far away from each other (i.e., source to destination consists of multiple hops), then more malicious nodes can interact in between source and destination. However, our approach produces higher PDR values than other two approaches.

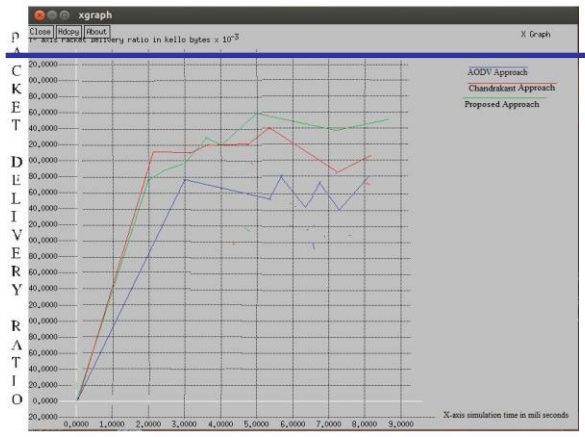

Fig. 2. Packet Delivery Ratio Vs Simulation time

This is because the malicious nodes initially have very much energy difference with the actual nodes. After elapse of time, the malicious nodes enter in the network with different batteries (i.e., different energies). Hence energy of malicious node cannot be judged by Chandrakant approach so it degrades the performance of packet delivery in multi hop network.

Table 2. Simulation parameters

Network Parameters	Values
Simulation Time	50 seconds
Number of nodes	2 to 50
Link Layer Type	Logical Link (LL)
MAC type	802.11
Radio Propagation Model	Two-Ray Ground
Queue Type	Drop-Tail
Antenna	Omni antenna
Routing	LAEERP
Traffic	Video
Network Area	1000m x 1000m

Simulation results show that the delay in our approach is less as the number of hops increases when compared to Chandrakant approach and AODV approach. This is because the existing approaches will take much time to find the energy of the node. Also simulation results show that if intermediate nodes are busy with other source-destination pairs for communication, still our approach maintains the higher Packet delivery ratio than the existing approaches.

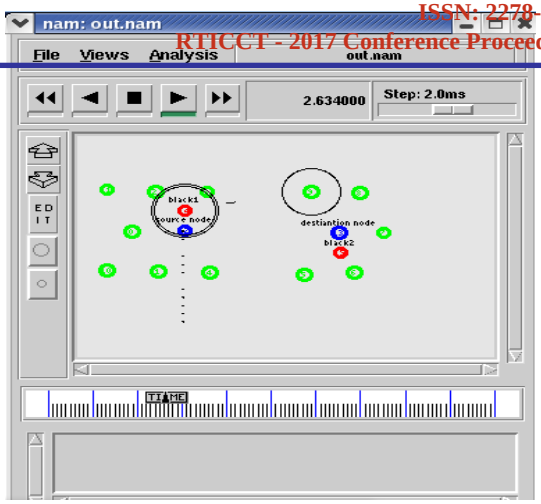

Fig. 3. (a) Blackhole detection

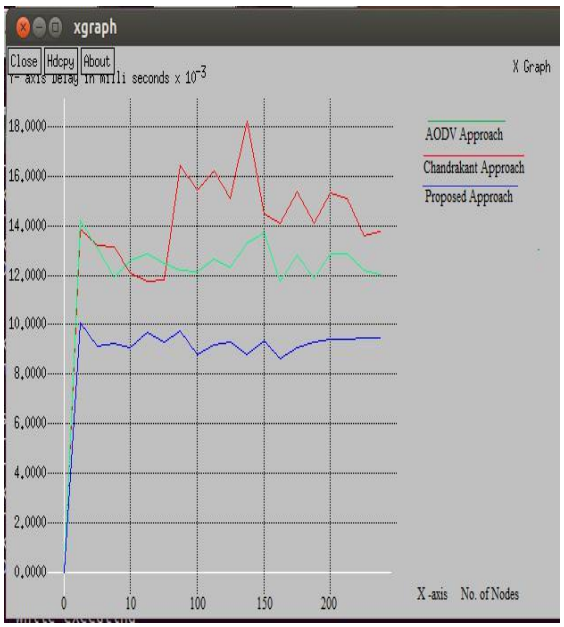

Fig. 3. (b) Delay Vs Number of nodes

V. CONCLUSION

In this paper, we use a concept of detecting Black hole attack in MANETs. The presented RCDM approach can easily detect the Black hole attack and also saves the energy and reducing the packet loss. Our approach guarantees the security against the Black Hole attack in MANETs. Our method performs well when compared to DSR. RCDM is a effective method in MANETs particularly when number of malicious nodes in the network is more and the nodes are having different energy levels.

REFERENCES

[1] Syed Jalal Ahmad, V.S.K. Reddy, A. Damodaram, P. Radha Krishna: Detection of Blackhole Attack using Code Division Method. Springer International Publishing Switzerland 34(5),(2015).

[2] Ahmad, S.J., Reddy, V.S.K., Damodaram, A., Krishna, P.R.: Location Aware and Energy Efficient Routing Protocol for Long Distance MANETs. International Journal of Networking and Virtual Organizations (IJNVO), Inderscience 13(4), 327–350 (2013).

[3] Chandrakant, N.: Self Protecting Nodes for Secured Data Transmission in Energy Efficient MANETs. International Journal of Advanced Research in Computer Science and Software Engineering 3(6), 673–675 (2013).
[4] Deng, H., Li, W., Agrawal, D.P.: Routing Security in Wireless Adhoc Networks. IEEE Communication Magazine 40(10), 70–75 (2002).
[5] Deswal, S., Sing, S.: Implementation of Routing Security Aspects in AODV. International Journal of Computer Theory and Engineering 2(1), 135–138 (2010).
[6] Hu, Y.C., Perrig, A., Johnson, D.B.: Aridane: A Secure On-Demand Routing Protocol for Adhoc Networks. Wireless Networks 11, 21–38 (2005).
[7] Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attacks and Counter Measures. AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols 1(2-3), 293–315 (2003).
[8] Lu, S., Li, L., Jia, L.: SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack. In: Proceedings of the International Conference on Computational Intelligence and Security, China, vol. 2, pp. 421–425 (2009).
[9] Neeraj Saini, Lalit Garg, A.: Enhanced AODV Routing Protocol against Black hole Attack. International Journal of Advanced Research in Computer Science and Software Engineering 4(6), 847-850(2014).
[10] Vipan Chand Sharma,Vivek Dimri," Detection of Black Hole Attack in MANET under AODV Routing Protocol", International Journal of Advanced Research in Computer Science and Software Engineering vol. 3 (2013).
[11] Harjeet Kaur, Manju Bala and Varsha Sahni, "Study of Black Hole Attack using different routing protocols in MANET". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol.2, Issue.7, (2013).
[12] Manjeet Singh and Gaganpreet Kaur, "A surveys of attacks in MANET". International Journal of Advanced Research in Computer Sciences and Software Engineering (IJARCSSE), Vol.3, Issue.6, (2013).
[13] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" Publisher ACM press, pp 96-97, (2004).
[14] Akanksha Saini, Harish Kumar," Effect of Black Hole Attack On AODV Routing Protocol In MANET",International Journal of Computer Science and Technology.
[15] R.Sudha, Dr. D. Sivakumar,"A Temporal table Authenticated Routing Protocol for AdhocNetworks",978-1-4577-1894-2011 IEEE.
[16] Yatin Chauhan, Prof Jaikaran Singh, Prof Mukesh Tiwari, Dr Anubhuti Khare," Performance Evaluation of AODV based on black hole attack in ad hoc network", Global Journal of researches in engineering Electrical and electronics engineering Volume 12 Issue 2 Version1.0 February 2012.
[17] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN 03), Las Vegas, Nevada, USA.
[18] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET", Journal Of Networks, Vol.3, No.5, May2008.
[19] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile AdhocNetworks: Simulation implementation And Evaluation, IJSEA, Vol2, No.3, July 2008.
[20] D Sheela , G. Mahadevan, Mollifying the Effect of Cloning, Black Hole Attacks in Wireless Sensor Networks using Mobile Agents, International Journal of Computer applications (0975 – 8887) Volume 55– No.9, October 2012.