Volume-7,Issue-6, (June-17)
ISSN (O) :- 2349-3585

DETECTING GRAY HOLE AND BLACK HOLE ATTACKS USING IDEA CRYPTOGRAPHY

N.Manohari[1],S.Radhika[2]
[1]Assistant Professor,[2]Research Scholar Department Of Computer Science, Theivanai Ammal College for Women, Villupuram,Tamilnadu,India

Abstract-The developments made in the computer technologies and wireless communication has led to the Mobile computing field. Mobile Adhoc Networks (MANET) is defined as the process of associating two or more nodes without seeking assistance from any centralized server. Hence, it is known as infrastructureless computing platform. This paper concentrates on detecting the black hole attacks and gray hole attacks via IDEA cryptographic model in MANET's environment. It is detected using Adhoc Demand Vector (AODV) protocol. The unique feature of AODV protocol is the dynamic response to discover the routes for better data delivery process. Black hole attacks are the attacks that claim the false routing information to the routing system whereas gray hole attacks do selective packet dropping at higher rate. Based on the neighboring node's information, the optimal routes are discovered. Then, the packets are transferred between the intended nodes. An experimental result will prove the effectiveness of the proposed algorithm. Performance metrics like throughput and routing overhead is analyzed which shows proposed IDEA scheme works better than the existing schemes.

Keyword: MANET, AODV, Hexagonal encryption, Black hole attacks and Neighboring nodes.

I.INTRODUCTION

A group of nodes that are independent and self- organized structure is known as wireless Adhoc networks [1]. Mobile Adhoc network is the subcategory of the wireless Adhoc networks. Mobile Adhoc Networks contain set of mobile nodes where the nodes are connected without use of routers or access points. When the source nodes transmit the data to its intended receiver, it can directly or indirectly i.e via intermediate nodes forwards the packets. The structure of the MANET is given in Fig.1 [2]. The procedure of generating the routes and then forwarding the packets to intended receiver is known as routing system. Due to the applications like military, battlefield and healthcare system, the inherent characteristics of mobile nodes are deployed [3].

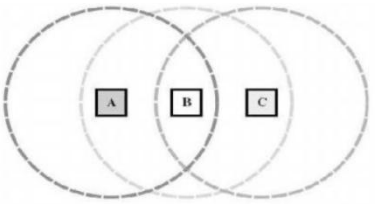

Fig.1. Structure of the MANET [4]

Generally, the routing protocol is classified into two sorts, namely, proactive routing protocols, hybrid and reactive routing protocols. Security is the major part of Mobile Adhoc Networks. Mobile networks are more prone to the malicious deeds. As mobile nodes move independently using mobile networks, it tends to continuous change in topology and route. Some routing protocols may be combination of above two protocols [5]. AODV protocol is the most widely adopted protocol that reduces the routing overhead. It provides free routes and repairs the broken links. Black hole attack is the most dangerous attacks that disturb the communications across the networks. Some control messages are used between sender and receiver node to establish the route [6]. The control message is of three types, namely, Route Request Message (RREQ), Route Reply Message (RREP), and Route Error Message (RERR).Adhoc On-demand Distance Vector (AODV) is the routing protocols that establish the communication path between sender and receiver with control messages. The rest of information fields hold the data like sender IP address, receiver IP address, sender and receiver sequence number, and hop count. With the help of this information, the packets are transferred between sender and receiver. By doing so, a routing table is maintained at every information transformation [7]. The RREQ message is broadcasted to all sensor nodes by the sender node. Based on

the acknowledgment from the sensor nodes, the packets are transferred under the transmission range. Then, the receive node sends the RREP message to sender node and thus the routing path is constructed. The sequence number of source determines the usage of route to its source node. Similarly, sequence number of destination determines the usage of route to its destination node.

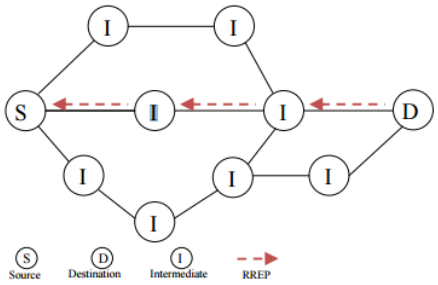

Fig.2. RREP message broadcasted to its intermediate nodes.

Route maintenance process is used for routing the process over a period of time. The 'Hello message' is transferred over the network to find the link failure. If any link failure is detected, then a notification is processed to its neighboring nodes. The source nodes then will decide whether to refresh the route or not [8]. Therefore, in order to fake AODV using Blackhole attacks, the attacker uses two methods:

• Send RREP packet towards the source node with highest enough sequence number.

• Send RREP packet to source node with small enough hop count number.

The rest of the paper is organized as follows: Section II describes the related work; Section III describes the proposed work; Section IV presents the experimental analysis and concludes in Section V.

II.RELATED WORK

The author in [8] studied about the selective forwarding attacks using checkpoints. The sensor nodes are randomly selected from its check point node. In accord to that acknowledgements are received and transmitted to its upper process. If any node didn't send the acknowledgments, then the warning message is generated. By doing so, the network cost overhead is reduced. The author in [9] was extended the same study by increasing the level of trust and packet loss. By removing the malicious node in the network, clustering method can remove the black hole attack [10]. The dynamic topology of the mobile network allows any node can join or leave the system. This scenario makes the system very tedious. The study was extended using artificial neural networks [11]. Black hole node(s) in the MANET and thus helps to minimize the smash up in reliable routing procedure. Black hole attacks are mainly applied to large scale applications [12]. The difference between normal node and malicious node is very much important in Adhoc networks. Some nodes may choose wrong path and thus data loss may occur [13]. The black hole attack is major problem for the wireless network and needs better solutions. In black hole attack the victim node sends the request for shortest path that leads its data towards destination [14]. The impacts throws by black hole attacks was studied by [15]. They proved that the black hole attacks have minimized conventional process. The author in [16] depicted a fuzzy based model to detect the black hole attacks. By minimizing the packet dropping rate, the malicious events can prevented. Every node in network transfers the packet based on the requests. Experimental results showed that the black hole attacks are determined at high positive rate. The author in [17] framed a novel method, named DPRAODV that segregates the malicious nodes from the network. An agent was used that transmits the destination number and determines the threshold value to estimate the training data. By processing so, every node in the neighbors gets actively participated and shares the information. The ALARM packet has the black list node as a constraint so that, the neighboring nodes know that RREP packet from the node is to be superfluous [18]. In additional, if any node receives the RREP packet, it looks over the list, if the answer is from the blacklisted node; no processing is done for the matching. It merely ignores the node and does not accept a reply from that node again. So, in this way, the malevolent node [19] is isolated from the network by the ALARM packet. They have compared the results with traditional AODV for simulation matrix like PDR and End-to-End delay [20].

III.PROPOSED WORK

This section depicts the proposed algorithm designed for detecting the black hole attacks and grey hole attacks using IDEA cryptographic schemes. The proposed algorithm

contains three steps which are explained as follows:

a)Topology Creation

Consider a sensor environment of 50 mobile nodes which are randomly distributed in 2000* 500 sizes. In accord to Poisson process, the nodes are randomly placed and forward the packets. A low traffic load is created among the nodes in mobile scenario. The speed range is from 5m/s to 2.70m/s. The transmission range is of 250m with data rate of 50kbps. Let us consider the data packets with payload information of 150 bytes.

b) IDEA cryptography

IDEA cryptography works in different from other cryptographic models. IDEA is the best known as block cipher algorithm. IDEA cryptography provides high level of security. Generally, the IDEA algorithm operates on 64bit plaintext and controlled by 128 bit key. The encryption process and decryption process is identical in nature. The IDEA algorithm steps are as follows:

i) The input block P of 64 bit is divided into four parts where each part contains 16bits.

ii) First round takes the input P1 to P4 that include eight rounds.

iii) The key size is of 128bits

iv) In each round, six sub-keys are used from original key which is of 16 bits.

v) Then the sub-keys are applied to the four input blocks.

vi) Thus, the first round contains six keys k1 to k6 and the eighth round contains k43 to k48.

vii) The process is continued until the four blocks of ciphertext of 64bits.

IDEA is a patented and universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. With a key of 128 bits in length, IDEA is far more secure than the widely known DES based on a 56-bit key. The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation.

c) Detection of Gray hole attack and black hole attack

Black hole attack is an attack that severely drops the packets using on-demand routing protocols like AODV. Malicious node acts as normal node and interrupts the routing process between sender and receiver. Similarly, the gray hole attack is an attack that operates on selective packet dropping process. Both of the attacks operate in routing layers. The transmission or dropping packets in the routing protocols on multiple nodes. Most of the attacker's intention is to disturb the routing protocols. Black hole attack cause more risks than the gray hole attacks. It is difficult to detect. Black hole attacks and gray hole attacks are found in virtual or wireless mesh networks. Gray hole attacks degrades the performance of mesh networks than the black hole attacks. In grey hole attack, the sender node receive reply message from malicous node and make smallest way to receiver node. Malicious node sends reply message after authorized node to sender node and then sender become confuse in two replies. On that way, malicious node becomes sender node and whole data received by it. In this, the data packets fully dropped by sender node. In the scenario, the sender node 1 sends large amount of RREQ message to every nearby nodes. When RREQ message is received by malicious node, then it sends RREP message to sender node which is non-real and also shows the shortest way to reach to receiver node. Then sender node accepts the reply message from non-real node which is called malicious node and transfers the packets.

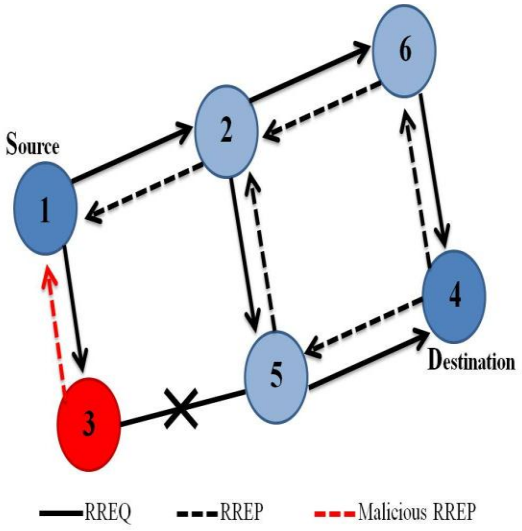

Fig.3. Proposed Architecture

IV.PERFORMANCE EVALUATION

This section depicts the experimental analysis of our proposed algorithm. The proposed IDEA cryptography is implemented using NS2, simulation tool.

ISSN:-2349-3585 |www.ijrdt.org

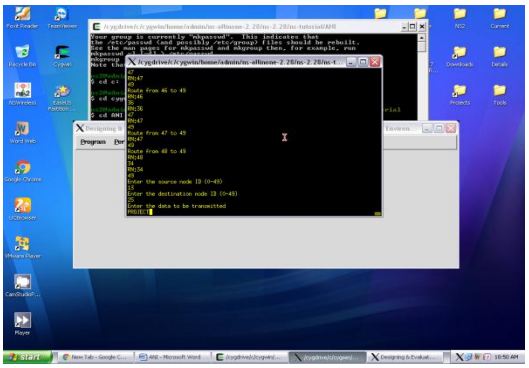

Fig.4. Initialization of source node and destination node

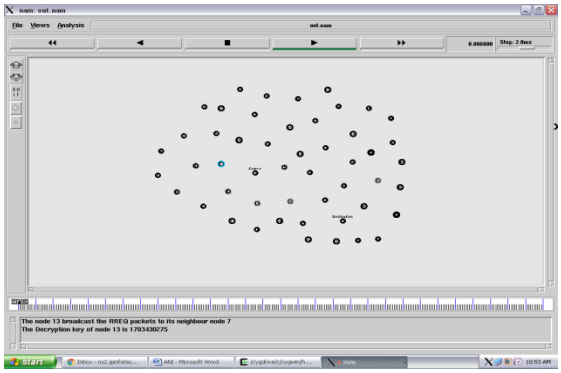

Fig.5. Node 13 sends RREQ messages to its neighboring nodes and collects the decryption keys.

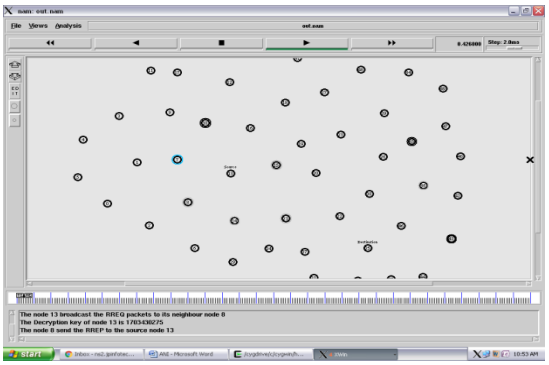

Fig.6. Node 13 sends RREQ messages to other neighboring nodes and collects the decryption keys.

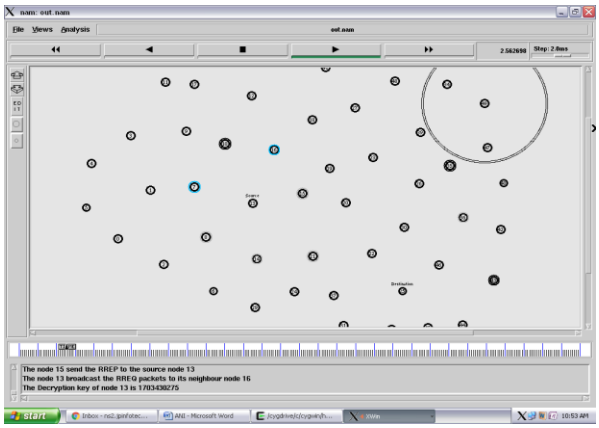

Fig.7. Node 15 sends RREP message to its source node 13 and collect its decryption key.

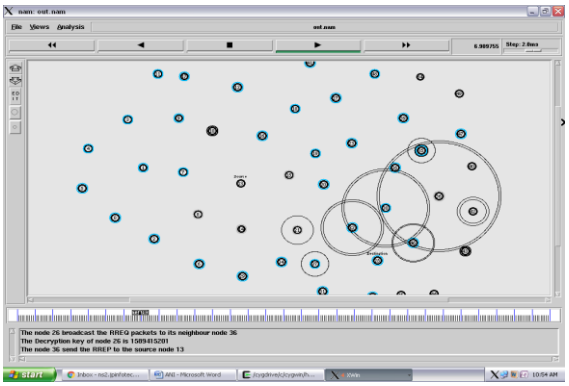

Fig.8. Similar process is done for all nodes in the sensor environment by forwarding RRREQ and receiving RREP.

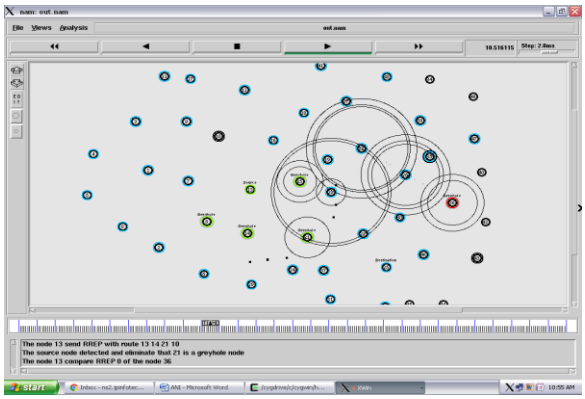

Fig.9. Node 13 sends the RREQ to its neighboring nodes and detects the gray hole attacks

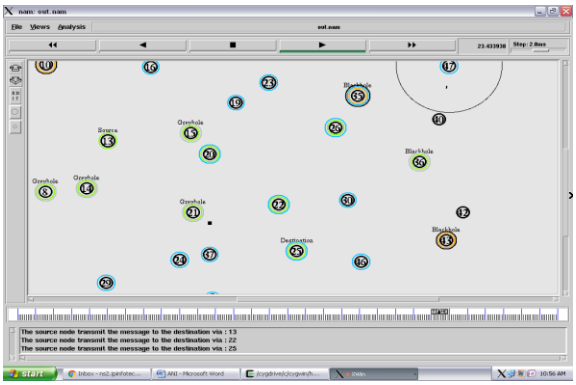

Fig.10. Detection of black hole attacks

Fig.11. Throughput comparison between existing and proposed system.

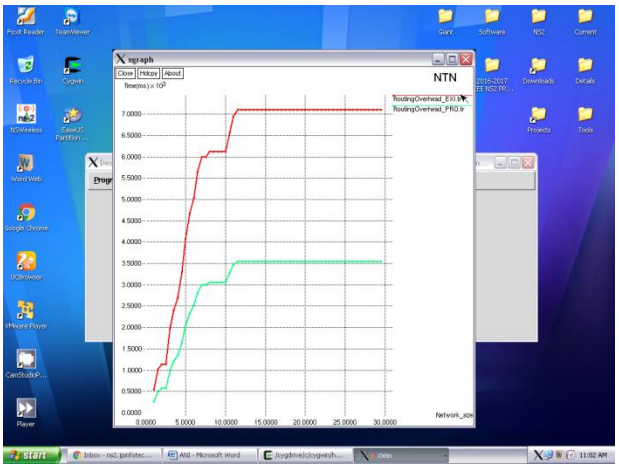

Fig.12. Routing overhead -Comparison between existing and proposed system.

V.CONCLUSION

Malicious behavior of the nodes affects the network performance to a greater extent. Thus, security plays a vital role in the mobile Adhoc networks. In this paper, we propose a novel IDEA cryptographic scheme that detects black hole and gray hole attacks in mobile Adhoc environment. There are various solutions proposed to address Black hole and Gray hole attacks but there is no one complete solution which addresses different varieties of Black hole and Gray hole attacks and provides a reliable, secure and efficient mechanism. The proposed model can be used to develop a technique that gives a complete solution to address these attacks and makes the data transmission reliable. Since, the encryption and decryption process is similar in nature. It makes data transmission as reliable and scalable one. Our future work aims to detect other types of attacks using the proposed model.

REFERENCES

[1] S. Balamurugan et al, "Black Hole Detection in AODV Using Hexagonal Encryption in Manet's", International Journal of Modern Engineering Research (IJMER), 4(12, 2014.

[2] Mr. Kumar Pradyot Dubey, Er. Kuntal Barua, "A Review - Techniques to Mitigate Black/Gray Hole Attacks in MANET", Engineering Universe for Scientific Research and Management (International Journal), Vol. 6 Issue 6 June 2014, 1-5 Paper ID: 014/EUSRM/6/2014/9046

[3] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011 (7-12)

[4] Saloni Sharma , Anuj K Gupta, " Survey of Secure mobile adhoc routing protocols", International Journal of Research in Computer Engineering and Electronics. 1 VOl : 3 ISSUE :2 ISSN 2319-376X ICV 4.08 IJRCEE@2014 http://www.ijrcee.org

[5] Rashmi, Ameeta Seehra, " Detection and Prevention of Black-Hole Attack in MANETS", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Jul-Aug 2014, ISSN: 2347-8578 www.ijcstjournal.org Page 204-209

[6] Athira V Panicker, Jisha G, "Network Layer Attacks and Protection in MANET- A Survey", Athira V Panicker et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3437- 3443

[7]Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", IEEE 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 978-0-7695-4336-9/11

[8]Garima Neekhra, Sharda Patel, Ashok Varma, "A Literature Review on Detection of Gray Hole Attack in MANET AODV Routing Protocol", International Journal of Emerging Technologies and Engineering (IJETE) Volume 1 Issue 7, August 2014, ISSN 2348 – 8050, 186-189

[9]V. Shanmuganathan, Mr.T.Anand, "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No6, December 2012, 647-650

[10]G.Vennila, Dr.D.Arivazhagan, N. Manickasankari, "Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm", G.Vennila et al. / International Journal of Engineering and Technology (IJET), ISSN : 0975-4024 Vol 6 No 5 Oct-Nov 2014 2401-2405

[11]Rohini Sharma, Meenakshi Sharma, "A Technique To Establish Shortest Route In MANET By Detecting Multiple Cooperative Black Hole Attack", Proceedings of IRF

International Conference, Bangalore 23rd March- 2014, ISBN: 978-93-82702-68-9

[12] Ms. Gayatri Wahane, Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack In MANET", International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014) 59-67

[13]Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", 1-4244-0983-7/07/$25.00 ©2007 IEEE ICICS 2007

[14]Vandna Dahiya, Ajay Dureja, "Detection of Black Hole & Gray Hole in MANET", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014, ISSN 2320–088X, pg. 466-473

[15]Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012, 37-41)

[16]Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[17]Perkins, E. B. Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," RFC: 3561, Nokia Research Center, 2003

[18]D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draftietf-manet-dsr-09.txt

[19]Mahmood, R.A., Khan, A.I.: A Survey on Detecting Black Hole Attack in AODVbased Mobile Ad Hoc Networks. In: International Symposium on High Capacity Optical Networks and Enabling Technologies (2007)

[20] http://www.isi.edu/nsnam/ns/