International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 10, Oct 2016)

A Technique to Mitigate Cooperative Blackhole Attack in MANETS

Roma Chanchlani[1], Priya Saxena[2]

[1]M.Tech Scholar, [2]Asst. Professor, Sanghvi Innovative Academy, Indore,M.P., India

Abstract: **Ad-Hoc is a kind of short durational network that does not have any managing authority which can create a bunch of nodes that can communicate with one another with in a fixed range of transmission and it is infrastructure independent. Open nature of communication make it vulnerable for so many security threats. Cooperative blackhole attack is one of the severe security threat which not only destroy communication but also degrade the performance by dropping the packets. This paper consist the problem observation and mitigate the cooperative blackhole attack using advance hop-count mechanism. It is simulated and evaluated using NS-2.35 simulator.**

Keywords: MANET, Cooperative blackhole attack.

I. INTRODUCTION

MANET is a less infrastructure network with vigorously changing topologies and arbitrary communicating node. At this time the mobile nodes communicate directly with additional nodes without any router and hence the preferred functionalities are embedded to each node. Since the MANET consists of mobile nodes with fewer configurations of hardware and requirements compared to a router, hence protocols and routing used are of lightweight functionalities. The range of protocol in MANET is categorized in two types: Proactive and Reactive. This work deals with enhancing MANET security through intrusion detection system for the AODV reactive protocol. The nodes that work towards degrading the normal network performance are called as malicious or attacker nodes. The sort of traffic generated by such node is nasty and affects the lifetime of network and other performance factor.

Also the intruder's node aim towards modification of actual packet information and forge them for diverting the network traffic through these malicious nodes which later on dropped or delayed. Hence, such intruder's nodes need to be identified timely for making the safe and secure communication in the network. For the period of the last few years, many approaches had been suggested along with several intrusion detection systems. Though there are some problems which remain unaddressed and are not resolved as required. In the presence of these nodes or in delays of such detection the network performance gets down continuously. In this idea it proposes a novel scheme based on FBU-NDA (Feature Based Unified Node Data Analysis) for AODV in MANET. These scheme is capable of detecting the intruder's node by continuously analyzing the network parameters and getting the acknowledgement counts. It also serves as a regular monitoring which access the behavior of each node. Result evaluation and comparison makes the actual assessment of the suggested approach and proves to be improved than traditional approach.

There are so many types of ad-hoc networks which work on different phenomenon's and transmission ranges such as Mobile Ad-hoc Network (MANET), WSN, WMN, Bluetooth, cognitive, VANET etc. In which each node will serve and support for data transfer. It does not have any controlling or monitoring head for managing this communication. Rather than that each and every node will do the same. So, the work specifically focuses its intensions towards making MANET more secure and robust.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 10, Oct 2016)

Ad-Hoc network is formed for the purpose of communication between the movable nodes such as laptops, cell phones tablets etc. As show in below Figure 1.1

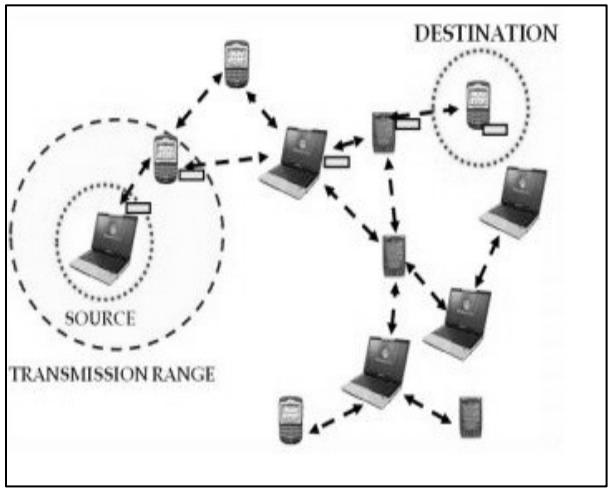

Figure 1.1 Mobile Ad-Hoc Networks.

They do not require any specific infrastructural needs for achieving this behavior. In such, WLAN (Wireless Local Area Network) gives the correspondence over the air with RF innovation without any physical association in the LAN based communication. Since the new standard presented in the remote neighborhood is one of most extreme issue behind developing enthusiasm toward open security correspondences have made new requests for solid transmission of continuous media for remote correspondence, 802.11 b. After the presentation with this standard remote neighborhood are more dependable as contrast with wired LAN as far as the information exchange and execution. The 802.11 b depicts the norms for physical and information connection layer. It utilizes IEEE 802.3 convention connection control, which is a piece of Data connection layer, (there are two sections in information connection layer one is intelligent connection control and other information connection control).

So every node treats as a router and executes a structure which is adaptive or non-adaptive in nature. So we can say that it can vary as the mobility of node grows. Nodes comes under a specific range will communicate directly with the help of remote connections, but they are far separated to use different hubs as transfers. These nodes generally transfer the same physical media. It can transmit and execute signals at the even frequency band by the total available bandwidth. By this transmission is easy and does not dependent on the network where vulnerable can be occurred due to the security policies are not properly executed for such a short range network. The chances of attack are more in MANET as comparison to any other wired network.

II. PROBLEM DEFINITION

With existing IDS it is very difficult to distinguish between normal traffic and intruder's activity traffic. Subsequently, Cooperative Blackhole is the group of malicious nodes deployed with mindset to increase the strength of malicious nodes. Thus the mechanism needs to be more productive to preempt those data losses by malicious nodes. In wireless network the connection is not static and mobile nodes can join and leave the network at any instance of time. On behalf of instance, a node which is in the short term out of synchronization may forward packets that could be considered of attack activities, IDS should use minimal resources that are not used in existing approaches. The current IDS mechanism is not able to detect several intruders node deployed with cooperative mechanism. Thus, this attacks need to be blocked. Data losses and identity theft by intruder's nodes is generally affected by lack of central monitoring points. Many other problems like, uncertain collisions, recipient collisions, restricted transmission power (Links & Resources), false misbehavior report and Collision are the entities not been managed by existing system.

After analysis the various research articles this work had identified following area of work which remains unsolved by existing IDS mechanisms. Compared with wired networks, where traffic monitoring is usually done at networking devices such as switches, routers and gateways, In MANET the mobile IDS should employment with localized and partial data because the ad hoc environment does not have traffic concentration points where the IDS can collect audit data for the entire network.

Problem 1: In the existing mechanism cross validations of behavior of each node is not yet performed thus their parameter selection is also weak which not covers each aspect of intruder's measurement.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 10, Oct 2016)

Problem 2: Partial drops and corruption in packets is also not given by any approach which leads us incorrect detections which later on affects the transmission by malicious node behaving as intruders.

Problem 3: Strong strength attacks like cooperative blackhole attack are also not prevented by any mechanism.

Problem 4: False route updates and traffic pattern distortion is unavailable with existing approaches.

There are some more problems like: Packet collisions, partial transmission power (Links & Resources), Receiver collisions, false misbehavior report and Collision are the entities which are not handled by existing mechanisms.

III. PROPOSED SOLUTION

It detects the malicious misbehaving nodes having usual collisions and packet droppings. Such node also generates the faulty misbehavior report that they are behaving well in the network while in reality they are harming the network performance by packet dropping. Thus, effective and on time identification of these nodes is necessary. Such identification is quite a tough task as the actual traffic is been analyzed and after which the unreliable transmission is identified by comparing it with the exiting flow pattern. Thus helps in identification of false loss and flow. The proposed work will improve the deficiency of existing IDS which fails to detect the false misbehaviour timely. This work proposes an Advance Hop-Count Based IDS [AHC-IDS] for AODV protocol. It works on the basis of 4 modules. It starts with data gathering, categorization, processing and intimation. The above scheme is named as a [AHC-IDS] because in this a feature based node characteristic is analyzed and monitored for intruder's identification. [AHC-IDS] can be measured through a threshold for behavioral pre-emption.

The proposed scheme of is designed to resolve the weakness of existing Watchdog and Pathrater approaches.

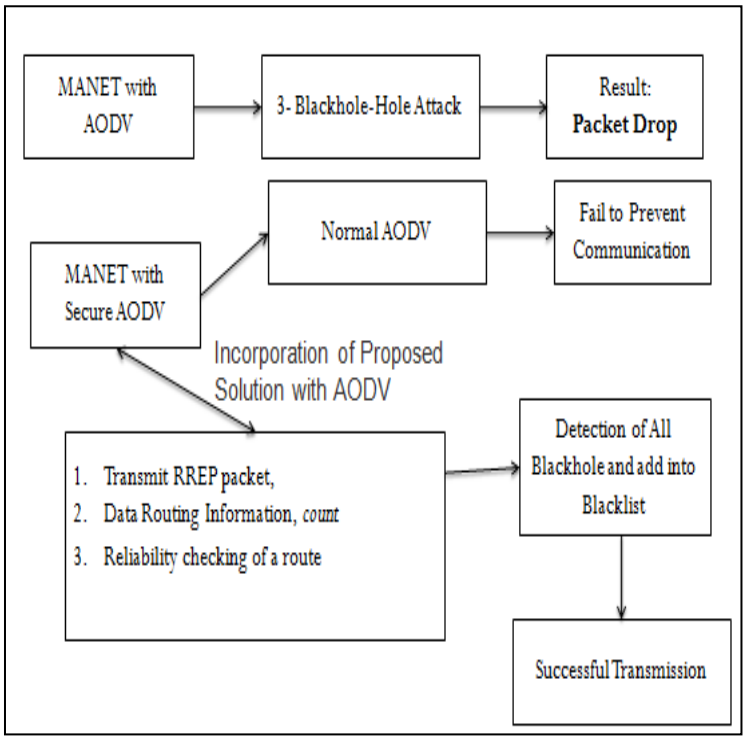

Figure 3.1: Proposed Advacne Hop-Count Based IDS

IV. IMPLEMENTATION & RESULT ANALYSIS

The following metrics are used in this work for comparing the performance of AODV, AODV under attacks and Modified AODV routing protocols.

1. Throughput
2. Packet Delivery Ratio
3. End-to-End Delay

Below Figures demonstrates the evaluated performance of normal AODV, AODV with cooperative blackhole attack and modified AODV with improved performance.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 10, Oct 2016)

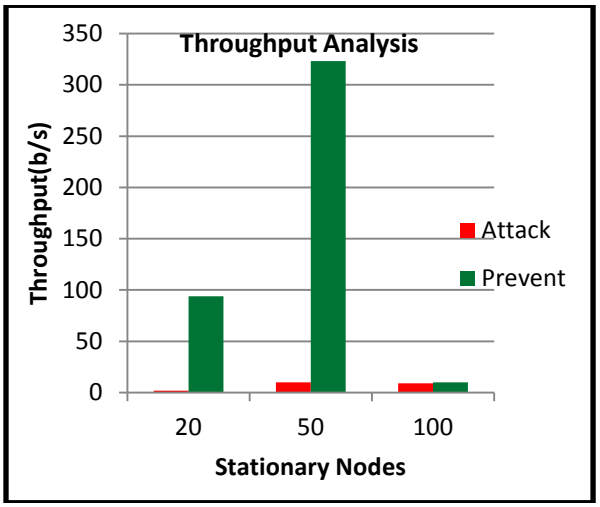

Figure 4.1: Throughput Analysis of Stationary Nodes

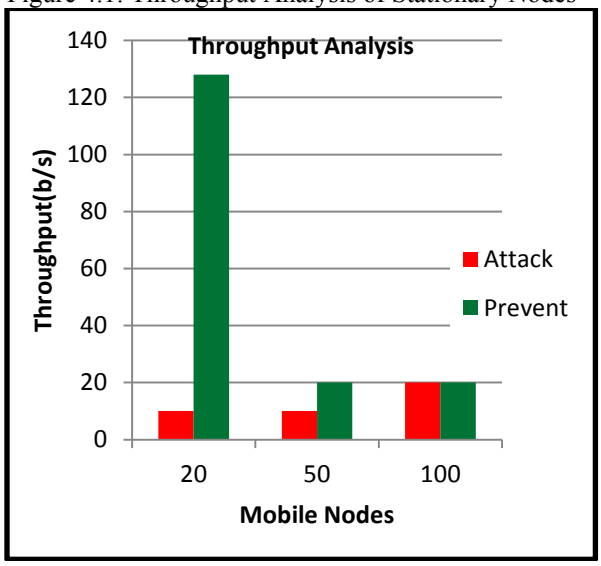

Figure 4.2 : Throughput Analysis of Mobile Nodes

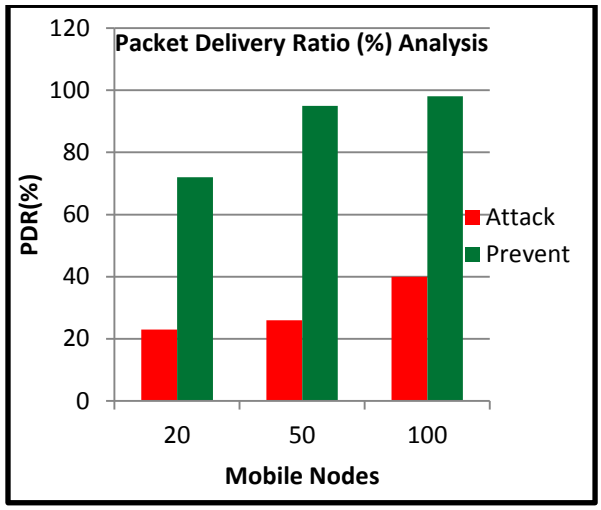

Figure 4.3 : PDR Analysis of Stationary Nodes

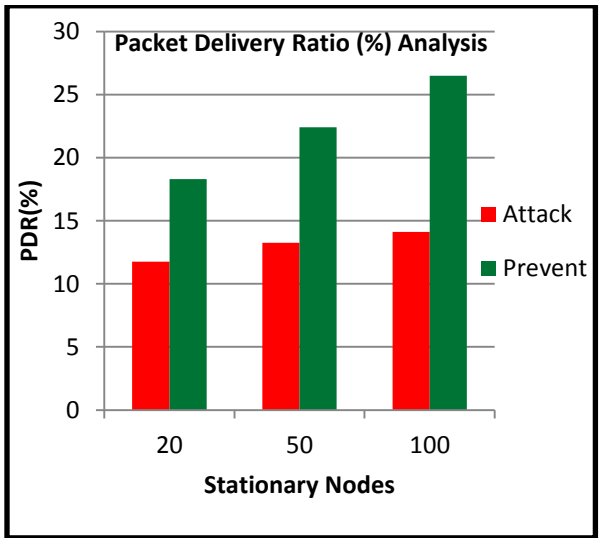

Figure 4.4: PDR Analysis of Mobile Nodes

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 10, Oct 2016)

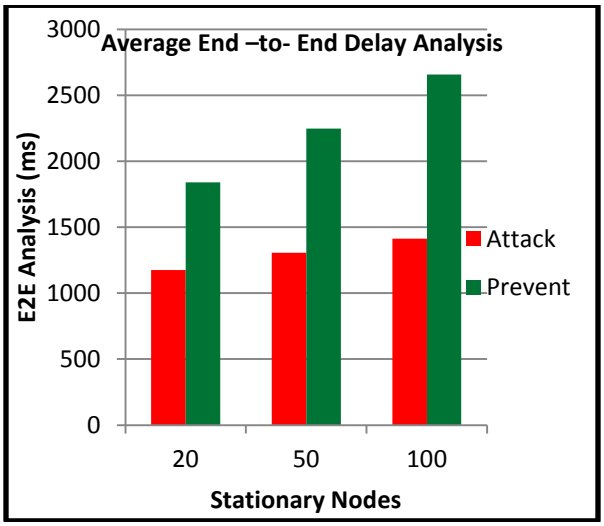

Figure 4.5:E2E Delay Analysis of Stationary Nodes

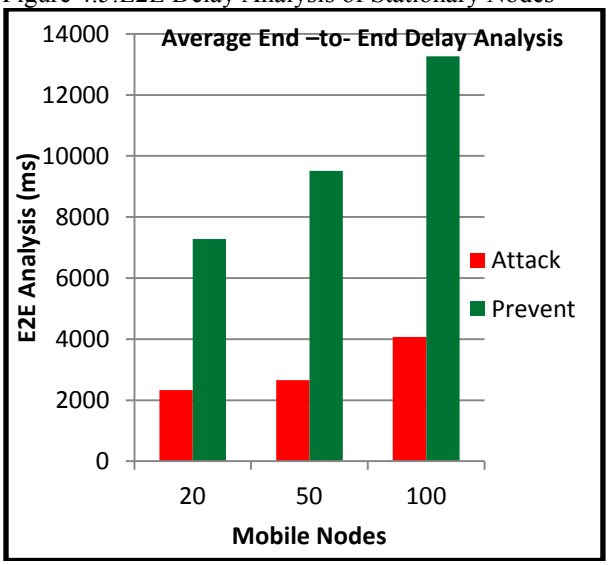

Figure 4.6:E2E Delay Analysis of Mobile Nodes

V. CONCLUSION

The complete simulation of attacking situation and proposed solution observed certain effect on mobile ad-hoc networks which is listed below;

1. Analysis of Figure 4.1 and 4.2 conclude that throughput of ad-hoc networks becomes well in proposed solution situation than attack. In case of stationary node 50 highest throughputs with 50 is achieved. Furthermore, 20 nodes ad-hoc network perform well in 20 node networks.

2. Packet delivery ratio is the measure observation for proposed solution. A very impressive packet delivery ratio is observed in both stationary and mobile state. For all kind of scenarios proposed solution gives better performance than attacking situation.

3. The major problem with proposed solution is extra overhead due to multi time hop count checking. Thus it gives poor performance in end-to-end delay parameter. Still, security always comes with overhead and it's all up to the requirement of security. So, if we want to prevent the network from cooperative blackhole attack we have to consider this end-to-end delay.

REFERENCES

[1] MarjanKuchaki Rafsanjani, Ali Movaghar, and FaroukhKoroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes", in World Academy of Science, Engineering and Technology, 2008.

[2]Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", in IEEE Transaction on Industrial Electronics, ISSN: 0278-0046, Vol. 60, No 3, March 2013.

[3] M Salman Ashraf1 and Muhammad Raheel2, "RGB Technique of Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 9, Issue 2, No 2, March 2012, pp 306-313.

[4] S.Mamatha and Dr A Damodaram, "Quantitative Behaviour Based Intrusion Detection System for MANETS", in Proc. of the Intl. Conf. on Advances in Computing and Communication (ICACC), ISBN: 978-981-07-6260-5 doi:10.3850/ 978-981-07-6260-5_59, April 2013.

[5] Umesh Prasad Rout, "A Study of Intrusion Detection Systems in MANETs", in International Journal of Research in Computer and Communication Technology, ISSN(Online) 2278-5841, Vol. 2, Issue 2, Feb-2013.S.Sasikala and M.Vallinayagam

[6] O. V. Chandure , A. P. Bakshi, S. P. Tidke and P. M. Lokhande, "Simulation of Secure AODV in Gray Hole Attack for Mobile Ad-Hoc Network", in International Journal of Advances in Engineering & Technology, ISSN: 2231-1963, Vol. 5, Issue 1, Nov. 2012. , pp. 67-76.

[7] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and ShaidahJusoh, "Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm", in IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[8] RakeshShrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han, "A Novel Cross Layer Intrusion Detection System in MANET", in IEEE International Conference on Advanced Information Networking and Applications, ISSN 1550-445X/10, DOI 10.1109/AINA.2010.52, 2010.

[9] Secured Intrusion Detection System in Mobile Ad Hoc Network using RAODV ", in Proceedings published in International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, ICRTCT-2013.

[10] Sagar Pandiya, Rakesh Pandit and Sachin Patel, "Survey of Innovated Techniques to Detect Selfish Nodes in MANET", in International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), ISSN 2250-1568, Vol. 3, Issue 1, Mar 2013, 221-230.

[11] S. P. Manikandan and Dr. R. Manimegalai, "Evaluation of Intrusion Detection Algorithms for Interoperability Gateways in Ad Hoc Networks", in International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 3 No. 9 September 2011.

[12] Tushar Sharma, MayankTiwari, Prateek Kumar Sharma, Manish Swaroop and Pankaj Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 3, March-2013.