DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5487

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PERFORMANCE COMPARISON OF BLACK HOLE ATTACK DETECTION MECHANISM IN 6LOWPAN OVER MANET

R.Sujatha
Ph.D. Research Scholar,
Dept. of Computer Science,
MaruduPandiyar College, Thanjavur ,
Tamilnadu,India.

Dr.P.Srivaramangai
Associate Professor,
Dept. of Computer Science,
MaruduPandiyar College, Thanjavur,
Tamilnadu,India.

Abstract: Black Hole Attack is the most vulnerable attacks in the network layer of wireless environment. In MANET, the existing techniques were proposed to detection and mitigate the black hole attacks. Thus the environment of the MANET which is differs from the 6LoWPAN Network. The cluster based nodes are connected together to form an MANET and also these type of architecture may have used in the 6LoWPAN Network. In MANET, it should be connected with the environment of mobile nodes itself rather; in 6LoWPAN architecture the mobile nodes are connected to form a network and also the nodes in the clusters can be connect with the internet through the gateway. The severity of attacks may differ from the environment to environment. Thus the malicious nodes may vulnerable within the range of MANET. It only can be able to connect with the nodes in the MANET rather it is most vulnerable thing is to detect the black hole attack from the nodes which are connected with the internet through the gateway. In this cluster based routing protocol implementation is proposed and the performance of the black hole attack detection can be analyzed and comparatively discussed with their results based on the parameters such as positive detection rate and energy consumption for packet overhead in the attack detection.

Key Terms: MANET, 6LoWPAN Networks, Network Layer Attacks

I. INTRODUCTION

Network Layer Attacks [1] [2] [9] are the most vulnerable to the networks those who are make self configuring on the demand of communications. In this case, the network layer attacks make worse when it should be very large and unproductive. In this network layer attacks, the vulnerability can be vary from the environment to environment. Thus the data packets can be discarded or dropped when the communication can be done based on the multi hop networks.

In MANET, the low power devices are connected together to form a network if it is multi channel and multi hop wireless networks, then the vulnerability of the network layer attacks like black hole attacks are more vigorous. The most familiar techniques for the detection of black hole attack detection are DSR, AODV and MAODV. Moreover these techniques satisfy the detection and mitigation with high positive detection rate up to 98% PDR.

Here it is more concentration is required for the implementation of detection mechanism in the 6LoWPAN Networks. This network having most different capabilities with the limited power and it is connected to the internet always with the edge router or with the gateway. The vulnerability through the internet gateway can be possible to attack the data communication over the cluster based network.

In this proposed work, we implement a framework to accomplish and compare the detection techniques using positive and negative detection rate for detection of black hole attacks in 6LoWPAN and MANET environments.

The comparison results using detection rate can used to obtain the performance of the attack detection strategies in these environments. The main contributions of this paper are as follows. 1. Implement the black hole attack detection in MANET and 6LoWPAN Networks using novel proposed framework. 2. Compare the performance based on the obtained positive detection rate of the techniques.

II. RELATED WORK:

In this section, we obtain the existing works for the black hole attack detection techniques for both the environments such as MANET and 6LoWPAN Networks. However there is no existing works form comparing the techniques and standards regarding the network based detection techniques evaluation through the detection rate. Here we discuss the related works for the techniques used in the environments.

Akanksha Sain and Harish Kumar [1] were made a huge survey about the techniques for the detection of cooperative black hole attack in MANET for this purpose, they used the assumptions and corresponding simulation results for the performance analysis.

Fan-Hsun Tseng et.al [2] were surveyed the existing solutions and discussed the state of the art of routing methodologies and techniques used for the detection of both single black hole attack and collaborative black hole attack. They mostly concentrate on the discussion of route discovery process and malicious misbehaviors.

In [3], Rooshabh Kothari et.al were used to implement the DSR technique for route discovery and detection of black hole and worm hole attacks in MANET through the proposed EM-DSR as Enhanced Malicious DSR. In this existing work [4], V.H.La et.al were proposed an mechanism for detection for misbehavior nodes in the light weighted link in the 6LoWPAN Networks.

III. BACKGROUND KNOWLEDGE

A. Mobile Ad Hoc Networks:

MANET is a type of infrastructure less wireless networks that can change the locations and can able to make self configure on the fly. Here the devices together in this network are mostly mobile devices can able to send the data signal to the mobiles each other and they use the wireless signals to connect and send data with each other. Here all the nodes are connected with each other if it is in the range of the data signal.

Some MANETs are constrained to a local area of wireless devices, while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network) is a type of MANET that allows vehicles to communicate with roadside connection stations. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure interchange circumstances or keep track of trucking fleets. Because of the self-motivated nature of MANETs, they are typically not very protected, so it is important to be wary what data is sent over a MANET.

B. 6LoWPAN Architecture:

The recent trend in the wireless environment with the wide range of connectivity with low power devices is obtained through 6LoWPAN networks [9][10][11]. 6LoWPAN is concerning more things to the cloud. Low-power, IP-driven nodes and wide range of mesh network support make this technology a great preference for Internet of Things applications. As the full name imply like as follows: “IPv6 over Low-Power Wireless Personal Area Networks” – 6LoWPAN [5] is a networking technology or adaptation layer that allows IPv6 packets to be conceded efficiently within small link layer frames, such as those defined by IEEE 802.15.4.

The 6LoWPAN is an open standard distinct in RFC 6282 by the Internet Engineering Task Force (IETF), the standards body that defines many of the open standards used on the Internet such as UDP, TCP and HTTP to name a few.

C. Black Hole Attacks:

A black hole attack [3] [4] is one of the most vulnerable kind of network layer attack where the malicious node under threat obtains the route with finest sequence number and less hop count between the source and destination and subsequently overhears or drops all data packets.

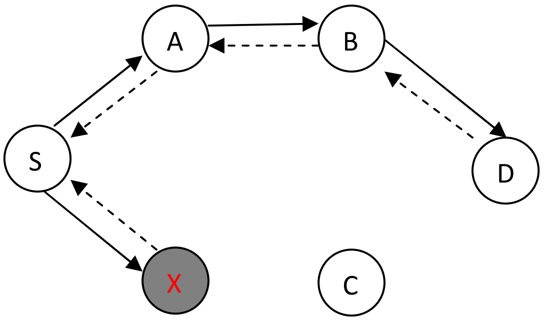

Fig 3.1. Black Hole Attack Illustration

The wide usage of MANET and 6LoWPAN [6] in hostile environment and other security perceptive usages have made the security a vital prerequisite for these networks. Because nodes participate in the routing process, they can destroy the network.

D. Black Hole Attack Detection techniques:

Most important and familiar techniques for the detection of black hole attack in MANET and 6LoWPAN Networks are divided into two protocols. They are Proactive and Reactive Routing Protocol. In these protocols, the recently used algorithms are from Reactive routing protocols such as AODV and DSR. AODV is constructed from the basis of DSDV Routing principles.

IV. Implementation

Here we implement the detection mechanism based on cluster based routing mechanism with the key management [6].

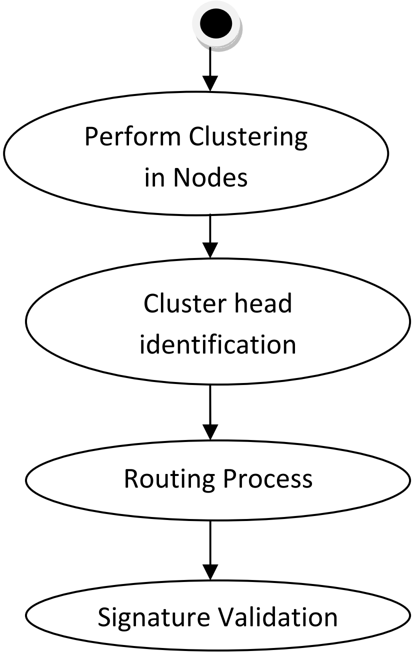

Fig.4.1 Work flow of proposed architecture of black hole attack detection

We propose this technique and implement it in the MANET [7] and 6LoWPAN architecture [9] to get the analysis of the performance of detection rate. We illustrate the work flow of detection mechanism through the figure as shown above. We use Matlab R2014b to implement the cluster based techniques of active nodes in the algorithm were we discussed.

IV. COMPARISON ANALYSIS

Here we compare the reactive routing techniques for the comparison of the black hole detection with the proposed cluster based techniques in the MANET and 6LoWPAN. The detailed implementation comparison can be done with the proposed work and the reactive routing protocols such as AODV and DSR are discussed and illustrated with the graphical analysis.

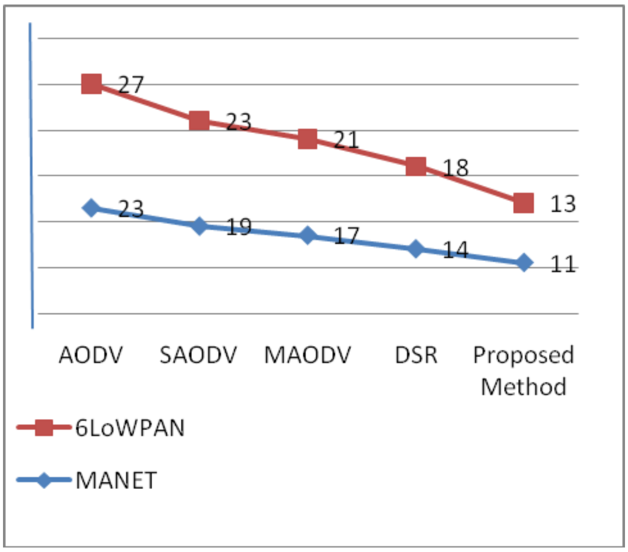

Fig 4.2 Comparison of Positive Detection Rate

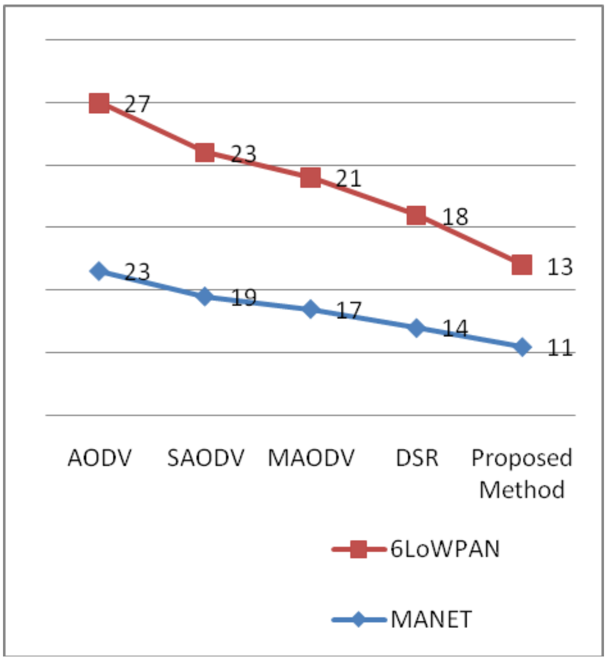

Fig 4.3 Comparison of packet loss

VI. CONCLUSION:

In this paper, the performance comparison for the implementation of black hole attack detection techniques AODV, MAODV and DSR in both the environments such as MANET and 6LoWPAN Networks. In this positive detection rate obtained for the techniques had used for the discussion over the comparison analysis. In future we compare the techniques with most vulnerable network layer attacks.

REFERENCES

[1] Akansha Saini and Harish Kumar, “Comparion between various Black Hole Detection Techniques in MANET”, NCCI 2010-National Conference on Computational Instrumentation, CIO Chandigarh, pp.157-161, March 2010.

[2] Fan-Hsun Tseng, Li-Der Chou and Han Chieh Chao, “A Survey of black hole attacks in wireless mobile ad hoc networks”, Springer Article in Human Centric Computing and Information Sciences, November 2011.

[3] Rooshabh Kothari and Deepak Dembla, “Implementation of Black Hole Security Attack using Malicious Node for Enhanced – DSR Routing Protocol of MANET”, Intl, Journal of computer Applications, Vol.64, No.18, pp.1-8, February 2013.

[4] V H LA and Ana R.Canavalli, “A misbehavior node detection algorithm for 6LoWPAN wireless sensor networks”, IEEE Intl. Conf. on Distributed Computing Systems Workshops, pp.49-54, 2016.

[5] Luis M.L,Oliveria, Joel.J.P.C.Rodrigues, Amaro D Sousa and Victor M.Denisov, “Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms”, IEEE transactions on Network Security, pp.2186-2195, August 2016.

[6] Yue Qiu and Maode Ma, “A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks”, IEEE Transactions on Industrial Informatics, Vol.5, No.12, pp.2074-2085, March 2017.

[7] Jain, S., & Hemrajani, N. 2013, “Detection and mitigation techniques of black hole attack in MANET: An Overview”, International Journal of Science and Research (IJSR), India Online ISSN- 2319-7064, vol.2, no.5, pp.70-73, May 2013.

[8] Divya R and Maheswari D, “Study of Various Security Attacks and in Network Layer and the Mitigation Techniques for MANET”, International Journal of Advanced Research in Computer and Communication Engineering”, Vol.5, Issue No.2, pp.404-410, February 2016.

[9] R Hummen, J Hiller, H Wirtz, M Henze, H Shafagh and K Wehrle, “6LoWPAN Fragmentation Attacks and Mitigation Mechanisms”, Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, Hungary, pp.55-66, April, 2013.

[10] A Rghioui, A Khannous and M Bouhorma, “Denial of server attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition”, Journal of Advanced Computer Science and Technology, Vol.3, No.2, pp.143-153, 2014.

[11] K Chugh, A Lasebae and J Loo, “Case Study of a Black Hole Attack on 6LoWPAN-RPL”, Securware 2012: The 6th Intl. Conf. on Emerging Security Information, Systems and Technologies, UK, pp.157-162, 2012.