ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Detection of Vampire Attack and Prevention in MANET

Harsha.N[1], Rashmi.S[2]

M.E (Pursuing), Department of C.E, Prof.Ram Meghe College of Engg and Management, Amravati, India [1]

Assistant Professor, Department of C.E, Prof.Ram Meghe College of Engg and Management, Amravati, India [2]

Abstract: Ad-hoc low-power wireless networks are the most promising research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of service at the routing or medium access control levels. Earlier, the resource depletion attacks are considered only as a routing problem, very recently these are classified in to a new group called "vampire attacks". Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing .It is clear that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. In this paper, we present an approach to detect and prevent the vampire attack in MANET.

Keywords: Vampire attacks, Ad-hoc low-power wireless networks, MANET etc.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. A large variety of MANET applications have been developed. For example, a MANET can be used in special situations, where installing infrastructure may be difficult, or even infeasible, such as a battlefield or a disaster area. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. The life of the wireless adhoc network depends on its node's battery power. In most of the applications, battery recharging or replacing is impossible. Power drainage will leads to the failure of the node and it will affect the network also. Data loss will also occur. Therefore an efficient energy utilization scheme is required, that is, data packets should be transmitted by using minimum units of energy. But some malicious packets called vampire packets may consume more energy for packet forwarding than that of honest packet forwarding .This will lead to power drainage of node and network failure. If we can find and avoid these type of vampire packets, then we can increase the life of the node and thereby the network.

II. LITERATURE REVIEW

Eugene Y. Vasserman and Nicholas Hopper describe the Vampire attacks in WSN [1]. Anoopa S and Sudha S K have proposed the methology for implementing detection and prevention in four phases, network layer vampire detection, Application layer vampire detection, Vampire handling and entropy and port scan details. Ambili M. A and Biju Balakrishnan [3] discuss an energy constraint intrusion detection scheme along with clean state secure routing protocol. A.Vincy, V.Uma Devi [5] discusses the energy efficient protocols that divide the network to efficiently maintain the energy consumption of sensor nodes. V. Rudoplu and T.H.Meng [6] described a distributed network protocol optimized for achieving the minimum energy for randomly deployed ad hoc networks. D.R. Raymond et al. [7] discuss the denial –of-sleep attacks at the MAC layer. S. Doshi, S. Bhandare, and T.X. Brown proposed the methology which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets[10][21]. J. Deng, R. Han, and S. Mishra describe the method to enhance survivability against denial of service (DoS) attacks[22]. A.J. Goldsmith and S.B. Wicker describe power-conserving MAC, upper layer protocols, and cross-layer cooperation [23]. Vidya.M and Reshmi.S explained about PLGP protocol which is mainly based on No-Backtracking property for depletion of vampire attacks [24]. Susan Sharon George and Suma.R explained the routing protocol to bind the damage caused by Vampires in the forwarding phase [25].

III. CONTRIBUTION

This paper makes two contributions. We present an approach which detects the vampire attack in MANET by fixing a particular threshold value and prevent the vampire attack by deleting the malicious node from the network.

IV. METHODOLOGY

In this paper, an approach is described to detect and prevent the vampire attack in Manet. In this approach our main task is to finding the malicious node during draining the battery life of the other nodes that are genuine and then

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

deleting that malicious node for the sake of improving our network and saving other nodes battery life. To detect the vampire attack in the network first we form a secure MANET i.e. user authentication is required to communicate with the other nodes. After user authentication is done the node can start the communication with the other users. When the node want to communicate with the other node it has to form a connection with that node by requesting for the connection. When the node request for the connection more that a particular count and the other node accepts the request with a particular session than the particular node is valid and the two nodes can communicate with each other. If that particular node does not accept that request in that particular session than that particular node is malicious node. When the node sends the request the malicious node will drain the battery life of that node till the battery life becomes very low. The node will not be able to communicate with the other nodes when vampire attack will occur. The malicious node will drain the battery life. To prevent the network from the vampire attack we will detect the malicious node and will delete the node from the network.

V. CONCLUSION

To conclude, we can say that the every technology has its impacts that include good impact and bad impact. It depends on our utility and use. By over viewing whole networking scenario we get the idea where we found that many malicious nodes are aiming to jam the network so that no one can able to make a connection with the others and no one can communicate with the others. They try to consume battery of the genuine nodes so that they cant be able to do make the connection So for avoiding all such things we present this approach for identifying the malicious nodes and get such malicious node deleted from the network.

VI. FUTURE SCOPE

In future the approach can be enhanced in various ways. Likewise by using this approach we can make Network traffic analyzer, network Jam Breaker, Node identifier. it can helpful for various telecommunication companies for maintaining their networks and for keeping their networks safe from the unauthorized access.

VII. ACKNOWLEDGMENT

We would like to thank all the people involved in research related in vampire attack in MANET & I like to thank my guide **Prof.R.P.Sonar** and **Dr.N.V.Thakur,** Dean of M.E Department.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless Ad-Hoc sensor networks", IEEE Transaction on Network Security for Technical Details, June 17, 2013

[2]. Anoopa S and Sudha S K," Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks", Int. Journal of Engineering Research and Applications, Vol. 4, Issue 4(Version 6), April 2014

[3]Ambili M. A and Biju Balakrishnan "Vampire Attack : Detection and Elimination in Wsn," International journal of scientific research, Volume : 3 | Issue : 4 | April 2014

[4] Gergely Acs, Levente Buttyan, and Istvan Vajda, "Provably secure on demand source routing in mobile ad hoc networks", IEEE Transactions on Mobile Computing 05 (2006), no. 11

[5].A.Vincy, V.Uma Devi" Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack," IEEE International Conference on Innovations in Engineering and Technology , Volume 3, Special Issue 3, March 2014

[6].V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp.1333- 1344, Aug. 1999.

[7].D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[8]. Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", IEEE workshop on mobile computing systems and applications, 2002.

[9]Andrea J. Goldsmith and Stephen B.Wicker, "Design challenges for energy constrained ad hoc wireless networks", IEEE Wireless Communications 9 (2002), no. 4.

[10]. S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002

[11]. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[12]. P. Papadimitratos and Z.J. Haas, "," Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002), Jan. 2002.

[13]. S. Marti et al., "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," Proc. 6th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2000), ACM Press, 2000, pp. 255–265

[14]Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.

[15] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, 2003.

[16]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

[17].K.Sivakumar and P.Murugapriya," Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks ," International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[18]. Mr. M.Rajesh Khanna, S.Divya and Dr.A.Rengarajan," Securing Data Packets from Vampire Attacks in Wireless Ad-Hoc Sensor Network," International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[19]. J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[20]. J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[21] Vidya.M and Reshmi.S," Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks," International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1, Issue 1 (March 2014)

[22]. Susan Sharon George and Suma.R," Attack-Resistant Routing for Wireless Ad Hoc Networks," International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014

[23]. Gowthami.M, Jessy Nirmal.A.G, P.S.K.Patra3," Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks ", International Journal of Advanced Research in Computer Science & Technology Vol. 2 Issue Special 1 Jan-March 2014