Scientific Journal Impact Factor (SJIF): 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Detection and Prevention of Energy Draining Attack in Wireless Ad-hoc Networks

Varsha M[1], Madesha M[2]

[1]*Department of Computer Science, SCEM*

[2]*Assistant Professor, Department of Computer Science, SCEM*

Abstract— Wireless Ad_hoc networks have become great interest in pervasive and sensing computing. In these networks batteries are used as the sole energy source. So energy efficiency becomes very critical. Due to ad-hoc organization, these networks are vulnerable to DoS attacks. One Type of DoS attack is Vampire Attack. Vampire attack is one of the resource depletion attacks. This kind of attack disables network communication by draining life of node's battery. This system is used to identify vampire attack in application layer. In this proposed system, detection and prevention strategy is used for vampire attacks, along with secure message forwarding method. For avoiding the entry of vampires from the network to packet, all the packets should satisfy no backtracking property.

Keywords— Wireless Ad-hoc Networks, Vampire attack, PLGPa, Security.

I. INTRODUCTION

Ad-hoc Wireless networks are the very promising research direction in sensing and pervasive computing. The Ad-hoc is used for wireless devices to communicate with each other directly. The Ad-hoc network does not rely on fixed infrastructure. This type of networks does not have a central access point. Each node can do routing. In Ad-hoc networks all devices have equal status on network. This network cannot connect to wired LANs or internet without installing special purpose gateway.

Ad-hoc networks refers IEEE.802.11 wireless standard. These networks are suitable in emergency situations like military conflicts, natural disasters. A wireless Ad-hoc network is a group of mobiledevices equipped with transmitter and receiver, which are connected without having fixed infrastructure. All the participating nodes are used for the control and coordination of wireless Ad-hoc network. Batteries are used for giving power to each node.

Wireless Ad-hoc networks are vulnerable to DoS Attacks. Denials of Service attack disable the network's capacity for performing normal operations. The most permanent DoS attack is resource depletion attack which drains node's battery power completely. Vampire attack is an instance of resource depletion attack. The vampire attack [1] can disables network communication by draining life of nodes battery power. That is vampire attacks consume more energy during message forwarding. The network is made up of multiple nodes. An energy based scheme is to detect the Vampire Attack should be implemented. Once a network is constructed, the vampire message will be send from the malicious node to any of the normal node. So the energy of normal node will be consumed more .Therefore we can conclude that the node is malicious node. Once the node is identified as the malicious node, the node is deleted from the network. Hence the vampire node cannot communicate with another node in the Network. The objective of this paper is to detect and prevent vampire attacks in wireless Ad-hoc networks. The vampire attack is more difficult to detect and affect slowly the networks then disable the networks.

II. RELATED WORK

The Detection of Vampire attack is one of the most crucial tasks. There are numerous methods developed to improve energy efficiency of the Wireless Ad-hoc Networks.

In 2005, C. Pandana and R. Liu introduced keep connect routing algorithm for maximization of network capacity in energy constrained ad hoc network. This computes the weight of the node based on how many components are connected to this node. Node's weight can be thought as the importance of node. The proposed KC algorithm with flow augmentation or with Minimum Total Energy algorithm provide the good result such as maximum connectivity of network and increase the lifetime of network [8].

In 2006, Bryan, Parno, Mark Luk, Evan Gaustad and Adrian Perring [3] presented a Secure Routing Protocol for forwarding packets in Ad-hoc Wireless networks.The protocol is not require any special hardware. The drawback of this protocol is that they provide message delivery in the environment with active adversaries. In 2007, Michael Brown-eld [4] proposed the energy resource vulnerabilities at MAC level. Denying sleep effectively attacks each node's critical energy resources and quickly drains life of network. So a G-MAC protocol is suggested to control the sleep awake node's pattern. That deals with MAC layer depletion attack only.

In 2003, Kar, Kodialam, T. V. Lakshman and L. Tassiulas proposed routing algorithm for the maximization of network capacity in energy constrained ad hoc network [7]. G. Anastasi, M. Conti, M. D.Francesco and A. passarella proposed numerous energy conservation schemes in wireless ad-hoc networks. To reduce power consumption in wireless ad-hoc networks, they introduced three main techniques, data-driven approach, duty cycling and mobility [9].

In 2011, Shaojie Tang, Xufei Mao, Xiahua Xu and Huadong Ma [5] introduced on opportunistic method to minimize energy consumption by all nodes but this method does not consider routing level attacks. This is based on the broadcast transmission for expanding the potential forwarders that assist in the retransmission of data packets. Here nodes in the forwarder list are prioritized and the lower priority forwarder would discard the packet if the packet is to be forwarded by using a higher priority forwarder.

In 2000, Wendi Rabiner Heinzelman et al., [6] proposed Low-Energy Adaptive Clustering Hierarchy (LEACH) clustering-based protocol for minimizing energy consumption in sensor networks. In the conventional protocols, multi hop routing, direct transmission, static clustering and minimum transmission energy should not optimal for sensor networks. To solve this problem, LEACH uses localized coordination for enabling robustness and scalability for dynamic networks and incorporated data fusion in the routing protocol to minimize the amount of data while transmitting to access point. The results showed that the LEACH minimized the communication energy compared with minimum energy routing transmission and direct transmission.

In 2011, Subhankar Mishra et al., [10] introduced the energy efficient protocols that have significant impact on lifetime of the networks. The algorithm is suggested to minimize the rate of consumption of cluster heads. LEAD combined with energy efficient round scheduling is used for allocation of cluster head. To increase the lifetime of the networks the cluster heads are dynamically selected in a round schedule balancing.

In 2013, Eugene Y. Vasserman and Nicholas Hopper [1] proposed a definition of vampire attacks. Vampire attack is an energy draining attack that consumes more energy during packet transmission. They proposed detection of vampire attack at network layer. In this proposed system, we are detecting vampires at application layer. The routing protocols like Ariadne, SAODV, and SEAD does not protect from Vampire attacks . Initially PLGP protocol is used for packet forwarding. Later modified it to PLGPa. The proposed system uses PLGP protocol with attestation for secure forwarding of packets.

III. THE PROPOSED APPROACH

The Proposed system is designed to detect and prevent vampire attacks inside the node. Whenever a vampire has detected inside the node, we can eliminate it and can prevent further forwarding of the packet. To avoid entry of vampires from the network to any packet, every packet should satisfy the property of no backtracking. PLGPa [1] protocol is used for secure message transmission. The proposed system is summarized on Figure 1.

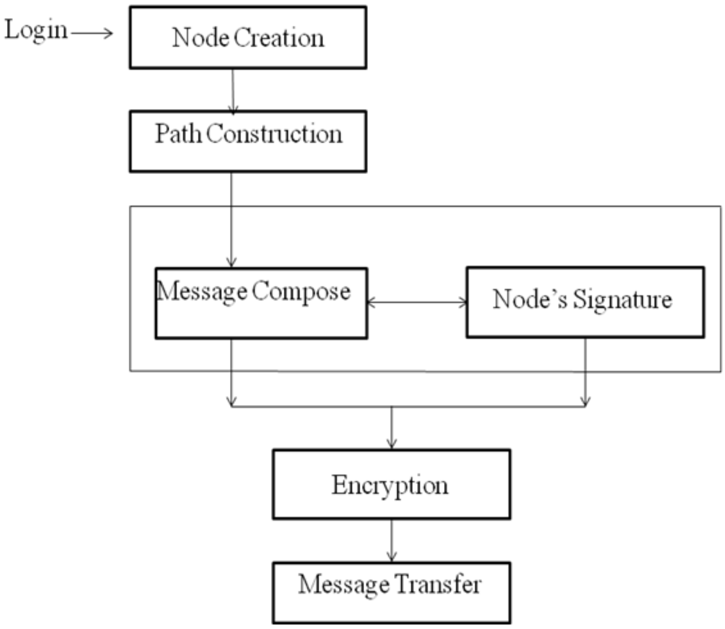

Figure 1. The Framework of the proposed system

Figure 1 depicts the architecture of the proposed system. Here the user will create the network i.e., create the nodes in the networks. Here user will select the sender node and receiver node from these nodes. Path is created by the Sender through which the packet has to be forwarded. Sender compose data and encrypts the data with sender's signature and sends to next Intermediate Node and finally to the Destination. If any vampire is detected inside a node, that malicious node is deleted immediately then stop the message forwarding.

If any vampire is present, then the consumption of energy will increase in abnormal fashion. The drainage of energy will leads to node failure and will disable the network.

IV.RESULTS

Energy attack (Vampire Attack) is a resource depletion attack that destroys battery power of nodes. In this proposed system a protocol is used for reducing the energy consumption effectively. The system provides more security for Wireless Ad-hoc Networks. This maximizes the lifetime the node's battery. It also increases the life of the network.

V.CONCLUSION

In this paper a detection and prevention method is introduced for the vampire attacks, which is a new class of resource consumption attacks that permanently disable ad-hoc wireless networks by draining nodes' battery power. The proposed scheme is to detect the vampire packets in the network and vampires inside the node. PLGPa algorithm is used to forward the packets safely in network. This system provides high security against the vampire attacks.

REFERENCES

[1] Eugene Y.Vasserman and Nicholas Hopper, "Vampire Attacks-Draining life from wireless ad-hoc sensor networks" IEEE Transactions, vol.12, No.2, February 2013.

[2] Anoopa and Sudha S.K, "Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks" International Journal of Engineering Research and Applications, vol.4,April 2014

[3] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perring", Secure sensor network routing: A clean-slate approach", CoNEXT, 2006.

[4] Michael Brown_eld,Yatharth Gupta, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of 2005 IEEE workshop on information assurance, June 2005..

[5] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy e_cient Oppurtunistic Routing in Wireless Sensor Networks", IEEE transactions on parellel and distributed systems, VOL. 12, NO.2, February 2011.

[6] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan "Energy-Efficient Communication Protocol forWirelessMicrosensor Networks," Proc. IEEE Transactions on, Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[7] kar, Kodialam, Lakshman & Tassiulas, (2003) Routing for Network Capacity Maximization inEnergy-constained Network, IEEE INFOCOM.

[8] Pandana & Ray Liu, (2005) "Maximum Connectivity and Maximum Lifetime Energy-aware Routing for Wireless Sensor Network," IEEE GLOBOCOM.

[9] Anastasi, Conti, Francesco, & Passarella, (2009) Energy conservation in wireless sensor networks: A survey, Ad Hoc Networks, vol. 7, No. 3, pp. 537-568

[10] Subhankar Mishra, Sudhansu Mohan Satpathy and Abhipsa Mishra "Energy Efficiency In Ad Hoc Networks " International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.1, 2011.

[11] 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.

[12] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks",International journal of computer applications(0975-8887)vol 40 No: 15,February 2012.

[13] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", IEEE GLOBECOM 2008,New Orleans,USA,December 2008.

[14] Vahid Shah-Mansouri and Vincent W.S. Wong" Distributed Maximum Lifetime Routing in Wireless Sensor Networks Based on Regularization"Proc. IEEE Transactions on, Ad-hoc and Sensor Networking Symposium, 2007.

[15] Seema Bandyopadhyay and Edward J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," Proc. IEEE Transactions on, Wireless Sensor Network, INFOCOM 2003.

[16] Rahul C. Shah and Jan M. Rabaey, Energy aware routing for low energy ad hoc sensor networks, Wireless Communications and Networking Conference, IEEE WCNC2002.

[17] Y.-C. Hu, D.B. Johnson, and A. Perring, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,"Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications, 2003.

[18] RoozbehJafari, FoadDabiri, and MajidSarrafzadeh"On Minimal Energy Skew Routing in Lossy Wireless Sensor Networks"Journal of Low Power Electronics, 1(2):97–107, 2003.

[19] Jae-Hwan Chang and Leandros Tassiulas, "Maximum lifetime routing in wireless sensor networks", IEEE/ACM Transactions on Networking 12 (2004).

[20] 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