Detection of Vampire Attack and Prevention for MANET

Harsha.Nanwani
M.E(Pursuing), Department of C.E , Prof.Ram Meghe College of Engineering and Management, Badnera , Amravati, India

Prof.Rashmi.P.Sonar
Assistant Professor, Department of C.E, Prof.Ram Meghe College of Engineering and Management, Badnera, Amravati, India

Abstract-
Mobile means able to move and ad hoc means transient without any fixed infrastructure so mobile ad hoc networks are a kind of transient networks in which nodes are able to move without any fixed infrastructure or centralized administration. Mobile ad hoc networks (MANETs) represent complicated dispersed systems that comprise wireless mobile nodes that can freely and actively self-organize into random and transient network topologies.

"Vampire-attack" is a kind of denial of service. The vampire attack is made by duelist node which makes energy consumption between nodes thereby draining the battery-life. So, the communication can't be framed properly and the packet transmission may not attain the goal. Vampire attacks are not protocol-definitive, in that they do not depend on design properties or implementation faults of particular routing protocols, but instead misuse general properties of protocol classes such as link-state, distance-vector, source routing, and geographical and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but instead try to send as little data as possible to achieve the largest energy drain, preventing a rate binding solution. Since Vampires use protocol-adaptable messages, these attacks are very difficult to detect and prevent

Keywords-Vampire attacks, Energy drain , MANET

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring structure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose” Each device in a MANET is free to move autonomously in any direction, and will therefore change its links to other devices repeatedly. Each must forward traffic irrelevant to its own use, and therefore be a router. The primary challenge in building a MANET is preparing each device to cohesively maintain the information required to properly route traffic A wide form of MANET applications have been created. For example, a MANET can be used in special situations, where installing structure may be complicated, or even infeasible, such as a battlefield or a disaster area.

The node's battery power decides the life span of a wireless adhoc network . In most of the applications, battery recharging or replacing is infeasible. Power drooping will leads to the failure of the node and it will affect the network also. Data loss will also occur. Therefore an skillful energy utilization scheme is required, that is, data packets should be send by using minimal units of energy. But some malicious packets called vampire packets may spend more energy for packet forwarding than that of actual packet forwarding .This will lead to power drooping of node and network breakdown. If we can detect and prevent these type of vampire packets, then we can increase the life of the node and thereby the network.

II. RELATED WORK

Ref. No.	Papers	Basic Concept	Performance Evaluation Parameter	Claims By Author	Our Findings
1	Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks	PLGPa is the Sensor network routing protocol that bounds damage from Vampire attacks	Bandwidth overhead is minimum	PLGPa bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations	The author has concentrated only in the network layer
2	Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks	Vampire packet (malicious packet) monitoring is performed both in network layer (routing protocol layer) and application layer.	Efficient energy utilization	The proposed methodology can be implemented as four phases, network layer vampire detection, Application layer vampire detection, Vampire handling entropy and port scan details.	Consumption of memory is more in the proposed methodology.
3	Vampire Attack : Detection and Elimination in Wsn	An energy constraint intrusion detection scheme is introduced along with clean state secure routing protocol	Efficient energy utilization	The proposed system describes some methods and alternative routing protocols solution that help to detect and eliminate vampire attack and thus make the network live	Using the proposed system, the nodes can find its neighbours that is nodes within its transmission range
4	Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks	Optimal energy boost-up protocol (OEBP) analyzes the routing table and verify the vampire attacks which permanently disable networks	Efficient energy utilization	This predicts the vampire attacks based on the existing behaviour and finds optimal path and optimal topology discovery.	Does not provide topology reconfiguration
5	Detecting and preventing vampire attack in wireless sensor network	Explains two attack on stateless protocol in which first is Carousel attack & second is Stretch attack.	Efficient energy utilization	Due to no backtracking property, the adversary cannot perform carousel or stretch attacks, no node may unilaterally specify a suboptimal path through the network.	Does not provide defences for topology discovery

III. PROPOSED APPROACH

The proposed approach describes the method to detect and prevent the vampire attack in MANET. In this approach our main work is to search the malicious node during draining the battery life of the other nodes who are genuine and then deleting that malicious node for the sake of improving our network and saving other nodes battery life. To determine the vampire attack in the network first we form a secure MANET i.e. user authentication is required to interact with the other nodes. After user authentication is done the node can start the interact with the other users.

When the node want to interact with the other node it has to form a connection with that node by asking for the connection. When the node ask for the connection more that a particular count and the other node accepts the request for connection within a particular session than the particular node is valid and the two nodes can communicate with each other. The node will send the request for connection to the other node for 3 times. For the first and second request it can directly accept the request .After that a response button will appear on the screen of the node which have to give the response to the node. If that node is busy then it can give response that "I am busy now" to the node than that node is true node.

Initially the battery level of the node is 100 units. When the node sends request, the battery level of that node will decrease by 10 units each time it will request for the connection. The node which request for the connection cannot communicate with the other nodes till the response does not come from the other node.

If that particular node does not accept that request in that particular session than that particular node is malicious node i.e it is not a honest node. When the node ask for connection to the malicious node,it will drain the battery life of that node till the battery becomes very low. The node will not be able to communicate with the other nodes when vampire attack will occur. The malicious node i.e the dishonest node will decrease the battery life of the node.

To prevent the network from the vampire attack we will detect the malicious node i.e the dishonest node and will remove the node from the network

- **Proposed System Algorithm**

The following is the algorithm of the proposed approach where Si denote the number of user, the threshold time considered is 10 units and count is the variable used to count the number of request .

❖ **Detection Algorithm for vampire attack:**

```
Step 1: Login with credential user s1
Step 2 : Authentication from server if not stop
Step 3: Send request s2 where ( s1,s2,s3…….
        sN) users
Step 4: s1 waiting for reply from s2.
Step 5:  if waiting_time > threshold_time and
         count++;
Step 6:  repeat step 3;
Step 7: else communication started
Step8:if count > threshold value attack
      detected
Step 9: else communication started.
```

❖ **Prevention Algorithm for vampire attack**

Step 1: Detect the malicious node using the detection algorithm.

Step 2: Remove the malicious node from the network

IV. IMPLEMENTATION

We have implemented the approach using Android .

❖ Using the proposed approach we can detect the vampire attack in the network.

❖ We can prevent the vampire attack by deleting the node from the network .

The following figure shows the comparison of energy .delay and throughput when there is an attack and after the prevention of vampire attack

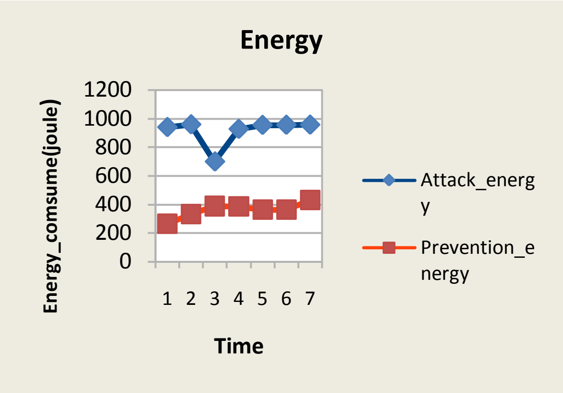

Fig : Comparison of Energy

The figure shows the comparison of energy when there is an attack and after the prevention of vampire attack

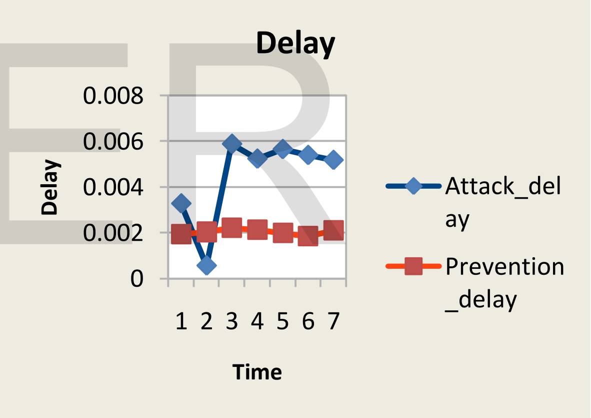

Fig : Comparison of Delay

The figure shows the comparison of delay when there is an attack and after the prevention of vampire attack

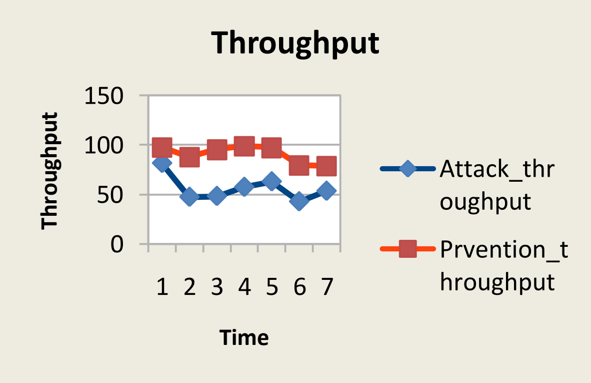

Fig : Comparison of throughput

The figure shows the comparison of throughput when there is an attack and after the prevention of vampire attack

V. CONCLUSION

Every technology has its impacts that include good impact as well as bad impact. It depends on the utility and use of the technology. By observing the whole networking scenario we get the idea that many malicious nodes are aiming to block the network so that no one can make a connection with the others and no one can interact with the others. They try to consume battery of the genuine nodes so that they can't be able to communicate with others. So for avoiding this we present this approach for identifying the malicious nodes and get such malicious node deleted from the network.

From the obtained results , we can conclude that, the proposed approach is efficient in terms of throughput and energy with the timely detection of vampire attacks in MANET

VI. FUTURE SCOPE

In future the approach can upgraded in various ways. Likewise by using this approach we can make Network traffic interpreter, network Jam cracker, Node identifier, it will be 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, H.O.D of CSE 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*DOI:10.1109/TMC.2011.274

[2]. Anoopa S and Sudha S K," Detection and Control of Vampire Attacks in Ad-Hoc WirelessNetworks", *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] 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*

[5] P. Lale, Dr. G.R. Bamnote" Detecting and preventing vampire attack in wireless sensor network", *International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 ,408-411*

[6] M.RajeshKhanna , 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*

[7].GergelyAcs, LeventeButtyan, and IstvanVajda,"Provably secure on demand source routing in mobile ad hoc networks",*IEEE Transactions on Mobile Computing 05(2006),no. 11*

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

[9]. 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.*

[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, "Secure Routing for Mobile Ad hoc Networks", *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]. YIH-CHUN HU, ADRIAN PERRIG," A Survey of Secure Wireless Ad Hoc Routing", *IEEE SECURITY & PRIVACY*

[16]. 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.*

[17]. 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)

[18]. 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*

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

[20].Soram Rakesh Singh*, Narendra Babu C R**,"** Improving the Performance of Energy Attack Detection in Wireless Sensor Networks by Secure forward mechanism", *International Journal of Scientific and Research Publications, Volume 4, Issue 7, July 2014*

[21] M.Mohana1, Kaviya.P**,"** A Survey on Secure Packet Transmission against

Vampire Attack in Wireless Ad-hoc Sensor Networks**",** *International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 11, November 2014*

[22].AnkitaShrivastava; RakeshVerma**,"** Detection of Vampire Attack in Wireless Adhoc Network**",** *International Journal of Software and Hardware research in Engineering,Vol.3 Issue 1 January*

[23]**.**Thanmanam. P , Suguna. M," DETECTION OF VAMPIRE ATTACKS USING OPTIMAL ENERGY BOOST-UP PROTOCOL IN WSN's",*International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014*

[24].JyotiThalor , Monika**,"**Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review**",***International Journal of Advanced Research in*

Computer Science and Software Engineering, Volume 3, Issue 2, February 2013

[25].Sureka.N, Prof. S. Chandra Sekaran," Securable Routing And Elimination Of

Adversary Attack From Manet",*International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014*

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

[27] 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*

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

[29]. 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.*

[30]. 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.*

[31] J. Singh, and N. Dhiman," A Review Paper on Introduction to Mobile Ad Hoc Networks*",International Journal of Latest Trends in Engineering and Technology (IJLTET)*
Vol. 2 Issue 4 July 2013 ISSN: 2278-621X

[32] G. Singh, J. Singh."MANET: Issues and Behavior Analysis of Routing Protocols",*International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012 ISSN: 2277 128X*

[33]A. Kumari , A. Kumar, and A. Sharma," Survey Paper on Energy Efficient Routing Protocol in MANET "*International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 3, March 2013 ISSN: 2277 128X*

[34] DonatasSumyla, Mobile Ad-hoc Networks, 03/20/2006.Available: http://ecom.umfk.maine.edu/MMobile%20Ad.pdf

[35] http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features

[36] PriyankaGoyal, VintiParmar, RahulRishi "MANET: Vulnerabilities, Challenges, Attacks, Application" *under IJCEM International Journal of Computational Engineering & Management, Vol. 11,January 2011 ISSN (Online): 2230-7893*

[37]http://en.wikipedia.org/wiki/Mobile_ad_hoc_network.

[38] Jun-Zhao Sun MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu, Finland "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing" under P.O.Box 4500, FIN-90014 University of Oulu.

[39] IETF Working Group: Mobile Adhoc Networks(manet).http://www.ietf.org/html.charters/manet-charter.html.

[40] https://www.techopedia.com/definition/5532/mobile-ad-hoc-network-manet