VAMPIRE ATTACKS IN WIRELESS SENSOR NETWORK –A SURVEY

Kirthika.K[1] , Mr.B.Loganathan[2]

1. M.Phil., Research Scholar, Department of Computer Science ,GAC , Coimbatore ,Tamilnadu.
2. Associate professor, Department of Computer Science, GAC, Coimbatore, Tamilnadu

Abstract: Wireless sensor networks plays a vital role in recent years . But those wireless networks suffers from lots of security threats. The proposal considers a new class of resource consumption attacks which is defined and named as Vampire attacks which is not clearly defined earlier in routing protocols and also vary under stateless and state ful routing protocols . Here network routing protocol prevents data from Vampire attacks by verifying packets consistently and makes progress toward their destinations with the verification and forwarding scheme .

Index terms: Wireless networks, Sensor network, Routing protocols.

Introduction:

Wireless ad hoc networks is a decentralized network which is a collections of wireless nodes connected by links which communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. They don't depend on a pre existing infrastructures and access points in managed wireless networks. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes. Ad hoc networks are vulnerable to Denial of Service (DoS) attacks which leads to the resource depletion. It also uses flooding for distributing data.

Vampire attacks are those new form of attacks on consumption of life from the network though they do not disrupt immediate availability, they work over time to disable the network entirely[2].

Vampire attacks are not specific to protocols as they do not depend on design properties of the particular protocol, but they are exploit to general properties of protocols such as link state and distance vectors.

ISSN: 2278 – 1323

Classification:

Classifying vampire attacks is most challenging as they use protocol complaint messages which makes them difficult to detect and prevent[6] .As vampire attacks are subject to DoS attacks they can be characterized by amplification and cumulative energy consumption[1] [6].

Vampire attacks causes more energy consumption while transmitting the message through the than if an honest node transmits the message with the same size[6].

Protocols:

Vampire attacks are mostly identified in link state, distance vector, source routing and Geographic and beacon routing protocols as well as logical ID based sensor network.

i)**link state protocols:** link state protocols which have the protocol OLSR optimized link state protocols uses the routing in two main classes such as Open Shortest Path First(OPSF) and Intermediate to Intermediate systems[3]. Basic concept of OLSR is that every node constructs the map for connectivity in between them.

ii)Distance vector protocols: Distance vector protocols are based on calculating the direction which means the next hop and the distance means the cost to measure the cost of next node[4]. The router inform its neighbor about the changes in the topology when the transaction in progress. It uses Bellman ford algorithm, and Ford Fulkerson algorithm to calculate paths.

iii)Coordinate and beacon based protocols are the protocols which moves according to the coordinates such as GPRS and BVR[5] [7][21]. In GPRS it contour the barrier of packets until to the path of target is reached whereas in BVR the packets are routed towards the beacon closest target and then move towards the target[6].

iv)Clean State Sensor Network routing: Clean state approach which are called PLGP in vampires[8]makes them vulnerable builds a tree shaped neighbor- hood used for addressing and routing at topology discovery and packet forwarding phase[6]

This can be further identified in on- demand routing protocols.

Types of vampire attacks:

Vampire attacks takes place in two different forms such as stateless protocols and stateful protocol.

i) **Stateless protocols**: Which treats each request as the independent transfer which are not related to any previous request. It simplifies the server design as it dynamically allocates the storage while transaction in progress .It is responsible for cleaning the server if the client dies in the middle. there are two different types of

ISSN: 2278 – 1323

attacks namely carousel attacks and stretch attacks.

Carousel attacks: In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. An example of this type of route is in Fig. 1[6]. The length of the adversarial path is a multiple of the honest path, which is in turn, affected by the position of the adversary in relation to the destination, so the adversary's position is important to the success of this attack[6].

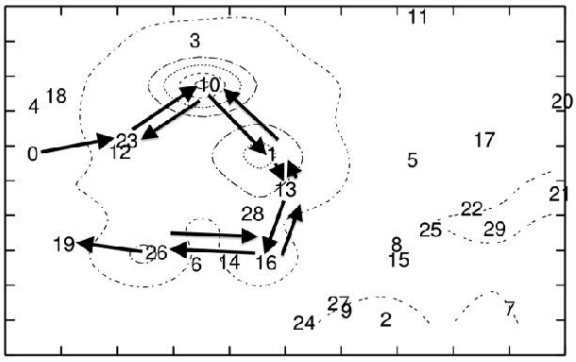

Fig 1:the nodes are transferred in a loop over all forwarding nodes roughly triples the route length

Stretch attacks: Stretch attacks targets the source routing protocols. An adversary constructs an artificial long routes, potentially transferring each node in the network causes the increase in the packet length and cause the packet to independent hop count along the shortest path. The stretch attacks depends upon the order of magnitude and depending upon the position of the malicious nodes. The stretch attacks will look as in fig2[6].

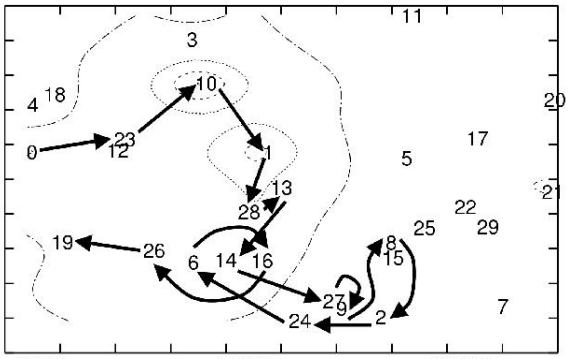

Fig 2: Route diverts from the optimal path between the source and destination.

ii)**Stateful Protocol:**

Stateful protocol are which able to remember and store details of the interaction between the nodes. It uses the two different protocols as link state protocol called OLSR[3] and distance vector protocols called DSDV[4].there are two types of attacks as follows

Directional antenna attacks Each node can waste energy by restarting a packet in various parts using directional antenna adversaries this attack can be considered as a half wormhole attack [9] as it constitutes the a private communication channel. packet

ISSN: 2278 – 1323

leashes cannot prevent this attack as they only protect intermediaries and not malicious messages[9].

Malicious discovery attacks: A malicious nodes has number of ways to induce a perceived topology charge in security measures as they proposed by Raffo et al in[10].this attack is trivial in open networks with unauthenticated routes of multiple nodes in neighbor relationship[11].packet leashes[9] cannot prevent these attacks as theses problems are same as BGP[12].

Securing vampire attacks:

An important part of securing vampire attacks includes No-backtracking. No-backtracking is satisfied when the packets are transferred in the same number of hops whether an adversary is present or not in the network[6].To preserve no-backtracking a verifiable path is added to the route authentication in Adriane[13]and path vector signatures[14].

The hop count of the packet received or forwarded by a honest nodes should not be greater than the number of entries packets In their route field[6].

Neighbor throttling can be limited in the number of way[15] or one way hash chain[14] and optimize discovery algorithm[18] can also be used to minimize the vulnerability of the vampires in windows.

Vampire flood its group using directional antenna snoop to merge the request from entire honest group and can be fooled easily.

In cryptographic accelerators are used for increased security demands on low power devices ,which leads to increased computational load and reduced battery life[16] ,[17],[39],[20],[49].

Carousel attacks can be prevented by forwarding node source check router for loops[6].Source roots cannot be corrected but it can be signed by itself[13].

A valuable secure protocol can be used in the network configuration phase to calculate the neighbor node to transmit faster[2].

Conclusion:

In this paper, Vampire attacks are those new form of attacks on consumption of life and energy from the nodes in the network .It has given the types of vampire attacks in stateless and stateful area and different protocol where the vampire attacks can be identified during the topology discover phase and packet forwarding can be secured using different techniques.

References:

[1]J.Bellardo and S. Savage, “802.11

ISSN: 2278 – 1323

Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security2003.

[2] K.Vanitha. and V.Divhya" A Valuable Secure Protocol to Prevent"Vampire Attacks In Wireless Ad Hoc SensorNetworks,2014

[3]T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.

[4] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. Conf. Comm. Architectures, Protocols and Applications, 1994.

[5] R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp. Networked Systems Design & Implementation (NSDI), 2005.

[6] Eugene Y. Vasserman and Nicholas Hopper"vampire attacks:draining life from wireless ad hoc sensor networks"2013

[7] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, 2000.

[8] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc. IEEE INFOCOM, 2001.

[9]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.

[10] D. Raffo, C. Adjih, T. Clausen, and P. Mu¨hlethaler, "An Advanced Signature System for OLSR," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN), 2004.

[11] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.

[12] C. Villamizar, R. Chandra, and R. Govindan, BGP Route Flap Damping, IETF RFC 2439, 1998.

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

[14] L. Subramanian, R.H. Katz, V. Roth, S. Shenker, and I. Stoica, "Reliable Broadcast in Unknown Fixed-Identity Networks," Proc. Ann. ACM SIGACT-SIGOPS Symp. Principles of Distributed Comput-ing, 2005.

[15] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.

[16] H. Eberle, A. Wander, N. Gura, C.-S. Sheueling, and V. Gupta, "Architectural Extensions for Elliptic Curve Cryptography

ISSN: 2278 – 1323

over GF(2^m) on 8-bit Microprocessors," Proc. IEEE Int'l Conf' Applica-tion-Specific Systems, Architecture Processors (ASAP), 2005.

[17] T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W.Marnane, "A Low-Power Pairing-Based Cryptographic Accel-erator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.

[18] Y. Huang and S. Bhatti, "Fast-Converging Distance Vector Routing for Wireless Mesh Networks," Proc. 28th Int'l Conf. Distributed Computing Systems Workshops (ICDCSW), 2008.

[19] M. Koschuch, J. Lechner, A. Weitzer, J. Groschdl, A. Szekely, S. Tillich, and J. Wolkerstorfer, "Hardware/Software Co-Design of Elliptic Curve Cryptography on an 8051 Microcontroller," Proc. Eighth Int'l Conf. Cryptographic Hardware and Embedded Systems (CHES), 2006.

[20] M. McLoone and M. Robshaw, "Public Key Cryptography and RFID Tags," Proc. RSA Conf. Cryptography (CT-RSA), 2006.

[21] R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp. Networked Systems Design & Implementation (NSDI), 2005

ISSN: 2278 – 1323