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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

A Survey on Secure Packet Transmission against Vampire Attack in Wireless Ad-hoc Sensor Networks

M.Mohana[1], Kaviya.P[2]

PG Scholar, Department of CSE, Sri Vidya College of Engineering & Technology, Virudhunagar, India [1]

Assistant Professor, Department of CSE, Sri Vidya College of Engineering & Technology, Virudhunagar, India [2]

Abstract: A wireless sensor network is a class of transducers which is used to monitor and record the conditions of a wireless environment. Denial of service is one of the common attacks in the wireless sensor network. Vampire attack is a kind of denial of service which consumes energy that leads to draining battery-life of the nodes in the network. Since the nodes are battery powered, the network lifetime is minimized. So communication between nodes cannot be made properly and also the packet does not reach the destination during transmission. This attack can be done by either extending the path of nodes or it may form a loop in packet transmission route. In this paper, we present various algorithms on secure packet transmission against vampire attack. This survey gives different algorithms to overcome the vampire attack and provide secure packet transmission in wireless ad-hoc sensor networks.

Keywords: Wireless sensor networks, Wireless ad-hoc networks, Denial of service, Vampire attack.

I. INTRODUCTION

A wireless sensor network consists of a number of sensors that are spatially distributed across a geographical area. An autonomous sensor forms a constitute network which is used for several applications. The applications are monitoring an environmental conditions, health-care monitoring, industrial monitoring, instantly deployable communication for military, power management, factory performance, on-demand computing power, smart sensing thereby information or data gathering and processing, inventory tracking, seismic detection and acoustic detection. Wireless sensor network consists of several characteristics like, mobility of nodes, ease of use, robustness, energy efficiency, heterogeneity, systematic design, scalability, responsiveness, self-configuration and adaptation.

A wireless ad hoc sensor network consists of a number of sensors deployed across a geographical area. Every sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. There are two ways to classify wireless ad hoc sensor networks. First, whether the nodes are individually addressable, and second, whether the data in the network is aggregated.

Due to Denial of service attack, the network may lead to performance degradation and loss of productivity. The attack can be done by adversary nodes. The aim of adversary nodes is to "resource depletion attack", by disabling the network which affects the communication path between nodes. It is one of the types of denial of service attack which causes damage to network by entirely depletes energy of node's battery-life.

"Vampire-attack" is a kind of denial of service. The vampire attack is made by adversary node which makes energy consumption between nodes thereby draining the battery-life. So, the communication cannot be made properly and the packet transmission may not attain the goal. The vampire attack can be done by two ways. The first attack is carousel attack which forms routing loops. Since, the malicious node sends packet in circle that allows a single packet to repeatedly traverse the same set of nodes which lead draining of battery life. The second attack is stretch attack; the adversary node can increase the length of path between nodes in a network. So the packet will travel along with unnecessary node instead of simple path to reach destination.

Those kinds of malicious nodes have to be identified to provide a necessary action to avoid these attacks. It can be done through route discovery and route maintenance process. The route discovery can be done by adding history thereby it will avoid carousel attack and route maintenance to make sure of security by performing the signature between communicating path nodes. The identified problem can be solved by newly-provable algorithm called "secure packet transmission".

Malicious nodes have injected necessary information or altering honest node's messages. For example, an attacker can forge messages to convince honest nodes to route packets in a way from the right destination. Vampire attack is also called as resource depletion attack. It mainly focuses on draining node's battery life which results that the network lifetime is reduced.

The rest of the paper is categorized as follows. Section II defines the vampire attack and its types. We discuss the various algorithms to overcome the vampire attack and provide secure packet transmission in Section III. Section IV finally concludes the paper.

II. BACKGROUND

A. Vampire Attack

Vampire attack is creating and sending messages by malicious node which causes more energy consumption. It

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

will lead to the depletion of node's battery life. Types of vampire attack are given as follows.

i. Carousel attack

Malicious nodes purposely introduced routing loops in a packet. This attack sends packets in circles. Its target is source routing protocols, allowing a single packet to repeatedly traverse the same set of nodes which forms a series of loops, so the same node appears in the route many times.

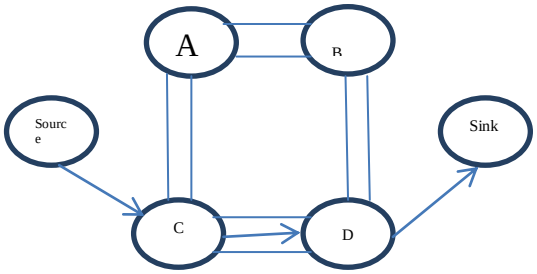

Fig. 1 Carousel Attack

ii. Stretch attack

The malicious node constructs artificially long routes, while traversing every node in the network. This attack increases a packet path length which causes a packet to be processed by a number of nodes that is independent of hop count along the shortest path between the malicious nodes and packet destination.

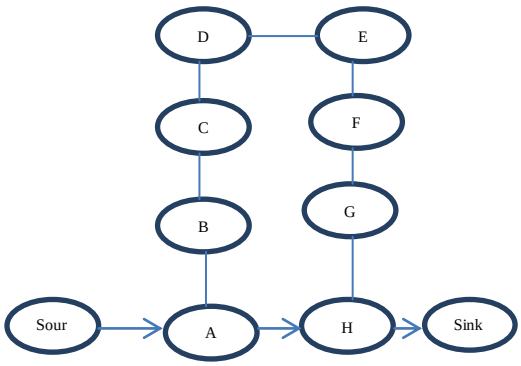

Fig. 2 Stretch Attack

III. ALGORITHMS

David Johnson**,** et al [1] proposed a new type of routing protocol called Ariadne that prevents the attacker in ad-hoc network. Here the compromised nodes tampering with un-compromised routes. Ariadne is based on DSR routing protocol which is applied to route discovery and route maintenance to avoid attacks and also provide security by means of one-time signature.

Gergely Acs, et al [2] described, a new source routing protocol "endairA" is used to provide security to prevent the attacks of malicious nodes. In EndairA, source node creates a route request that is broadcast to its neighbor node. In route discovery process an intermediate node can receive that request and appends their signatures that are rebroadcast to its target. The destination node creates a digital signature as a route reply that can be forwarded to source node. The given system provides security against the presence of an adversary.

David Johnson, et al [3] presented a new type of attack called "rushing-attack". The previously available protocol may fail under rushing attack and also they developed a new prevention method called "rushing-attack prevention". Here, the flag indicator is applied to resolve the problem of malicious nodes.

R.Sangeetha, et al [4] focused on energy available at each sensor node. A distinct vampire can shrink large enough usage on the whole network to drainage energy of nodes. All previous approaches are vulnerable to vampire attacks which are destructive, not easy to intellect and easy to carry out malicious insider sending protocol yielding messages. The implemented an approach "secure packet traversal" to achieve increased power consumption by effective nodes.

Santhosh L, et al [5] discussed a new version of vampire attack that disables an entire network permanently by quickly draining of node's battery power. Detection Algorithm is applied to each routing node in a network. If a node receives a packet it has to generate a signature for that packet and it is added to a list if they are not already presented. If the signature already exists in the list then the routing node will drop that packet.

Achuthan Ganthi, et al [6] considered worm-hole attack. Due to this attack the packet cannot reach to its destination. The packet forwarding can be done by AODV routing protocol. This protocol can identify the packet droppers. AODV routing protocol will identify the attacker node then find an alternative path to traverse a packet that the path should not have any kind of attacks. One more advantage of this protocol is to calculate the packet delivery ratio. They proposed a system which helps us to achieve reliable packet delivery and take only less time to traverse the packets. It identifies the route droppers before the transmission of the packets.

Bryan Parno, et al [7] evaluated a new secure routing protocol called "clean-slate approach" for sensor networks. The proposed model has focusing message delivery even in an environment containing with an active adversaries. They proposed a new sensor network routing protocol called Geographic hash tables (GHTS) and a key distribution scheme like PIKE with high security efficiency.

Chris Karlof David Wagner, et al [8] mainly focused on security issues in routing layer. They discussed how the ad-hoc and peer-to-peer networks can adopt to powerful attacks. They focused two types of attacks that are sink hole and hello floods. Link layer encryption and authentication mechanisms work with defense against malicious nodes.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Qing Cao, et al [9] considered a cluster. In cluster any node in next-hop can take forwarding responsibility that specially designed for wireless sensor networks. By using they achieved better energy efficiency and that will reduce retransmission. The result is efficient and improves end-to-end energy and latency of current routing protocols.

Chung Kei Wong, et al [10] presented a Feige-fiat-shamir digital signature scheme to speed up both signing and verification operations as well as they allowed adjustable and incremental verification operations. These operations are done through tree chaining techniques. The proposed signing and verification process (eFFS) is more efficient than DSA and Elgammal. An adjustable and incremental verification are more useful in large-scale multicast applications that work with a variety of receivers including limited resources.

Joongseok Park SartajSahni, et al [11**]** analyzed a lot of routing problem by on-line heuristics in wireless sensor network. In on-line models, each message has to be routed without knowledge of future route request. They developed an on-line heuristic that will maximize network life-time by performing two-shortest path computation for routing their messages. The capacity metrics are increased by using heuristic. The on-line maximum lifetime heuristic (OML) is used to maximize the network life-time that deals with delay depletion of sensor's energy nodes.

Youngsoo Kim, et al [12] proposed a new scheme to transfer an active packet to all neighboring nodes securely. They used public-key crypto system and asymmetric key crypto system. Lakshminarayanan, et al [13] provided two results to overcome attacks in the network. First, they provided a distributed algorithm that can achieve a reliable broadcast in an unknown fixed identity network even an adversary presence. Second, the problem of reliable broadcast in sparse network even if there is a single adversary present. They have developed decentralized security measures to protect internet against adversaries and achieved decentralized public key distribution in static networks.

M.BalaGanesh, et al [14] proposed 2-ACK scheme to send two-hop acknowledgement of packets in the opposite direction of the routing path. They designed a new intrusion-detection system called "EAACK" (Enhanced adaptive acknowledgment) that can detect highly malicious behavior rates and improve the network performance. The network problems can be tackled by EAACK. EEACK can also extend with digital signature to prevent the attacker from forging acknowledgement packet.

Sureka.N, et al [15] explored that at the routing layer, there is resource depletion attack which is also called "vampire attack". They discussed a method to moderate these types of attacks by including a new proof-of-concept protocol that provably bounds damage caused by vampire during the packet forwarding phase. In order to detect and eliminate the vampire attack, they implemented certain intrusion detection system. This mechanism is based on the energy level constraints.

Tarun Kumar Mishra, et al [16] ad-hoc network can help solving issues of attack from private nodes by authentication techniques that provide mutual trust between nodes. They also invoked digital signatures for security. They used AODV protocol to provide route on-demand and integrated many features to maximize performance at reduced routing overhead. Also they have added cost of complexity for efficient analyzes. They also included route availability and validation process.

MarcinPoturalski, et al [17] provided a basic variant of neighbor discovery problem. They have derived a protocol named as *time-based protocol and time-location based protocols*. The secure neighbor discovery process can be done successfully by using these protocols. The time based protocols are used to exchange a message between a set of nodes and to measure those nodes accurately with time factor. They proposed a framework which provides a secure neighbor discovery process with simple topology. This framework is also used to control a node's transmission power.

Sharon Goldberg, et al [18] designed and analyzed a new type of protocol called *path-quality monitoring protocol*. By using this protocol they were able to raise a reliable alarm when the packet losses or delay exceeds a threshold value. They proposed two technologies. Initially, secure sketching protocol invoked and it will identify the packet losses and delays. Finally, by invoking secure sampling protocols that makes a faster feedback and accurate round-trip delay estimates are done.

Amitabh Saxena,et al [19] presented one-way signature chaining which generates a chain of signature on the same message by different users. Here, each signature can act as a link. An intermediate node can be infeasible to remove links. This chain signature can be constructed by computational Diffie-Hellman (CDH) method. The chain signature is similar to transitive signature. It considered verification encrypted signature (VES) and sequential aggregate signature (SAS). . It also provides truncation resilience from that will distinguish it from other multiuser signature schemes.

Prosenjit Bose, et al [20] described a distributed algorithm for routing that do not require duplication of packet at node and yet guarantee packet delivery that are reached to its destination. This algorithm is also extended to yield broadcasting and geo-casting mechanisms. They described an algorithm that will broadcast and geo-casting in unit graphs. This protocol does not require any duplication of packets and it makes guarantee delivery of packets that are definitely reached to its destination.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

IV. CONCLUSION

Vampire attack is a resource consumption attack that use routing protocols to make a denial of service in order to disable entire ad-hoc wireless sensor network by drainage of node's battery life. In this paper, we discussed different algorithms to prevail over vampire attack and provide secure packet transmission. By avoiding these attacks, we can improve the lifetime of the network.

REFERENCES

[1] David B.Johnson, Yih-Chun Hu and Adrian Perrig,"Ariadne: A secure On-demand Routing protocol for Ad Hoc Networks *",InWireless Networks 11, 21–38,* 2005.
[2] GergelyAcs, LeventeButtyan, and IstvanVajda,"Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks",*IEEE Transactions on Mobile Computing,mar*.2005.
[3] David B.Johnson, Yih-Chun Hu and Adrian Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols ", *2nd ACM workshop on Wireless security*, 2003.
[4] R. Sangeetha, R.Deepa, C.Balasubramanian, " Provably Secure Routing and Defending Against Vampire Attacks in Wireless Ad Hoc Sensor Networks "*,IEEE International Conference on -ICIET'14,mar.*2014.
[5] Santhosh L, A.V.Krishna Mohan, "Prevention of Resource Depletion Attack in Wireless Sensor Network ", *5th Proceedings of SARC-IRF International Conference,* may.2014
[6] Achuthan Gandhi G and G. Vijayalakshmi, "Identification of Packet Droppers and Effective Routing of Packets in Wireless Sensor Networks", *International journal of technology enhancement*, 2014.
[7] Bryan Parno, MarkLuk, Evan Gaustad, and AdrianPerrig, "Secure Sensor Network Routing: A Clean-Slate Approach ",*Proceedings of the 2006 ACM CoNEXT conference2006.*
[8] Chris Karlof David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Article in Elsevier*, 2002.
[9] Qing Cao, TarekAbdelzaher, Tian He, Robin Kravets,"Cluster-Based Forwarding for Reliable End-to-End Delivery in WSN ", *IEEE INFOCOM*, 2007.
[10] Chung Kei Wong and Simon S. Lam,"Digital Signatures for Flows and Multicasts ", *IEEE transaction on networking,, VOL. 7, NO. 4,* aug.1999.
[11] Joongseok Park SartajSahni, "Maximum Lifetime Routing In Wireless Sensor Networks", *IEEE/ACM Transactions on Networking* 2005.
[12] Youngsoo Kim, Jungchan Na, Seungwon Sohn, "A secure method for transferring active packets*", Proceedings of WSEAS,* 1997.
[13] Lakshminarayanan SubramanianRandy H. KatzVolker RothScott Shenker Ion Stoica, "Reliable Broadcast in Unknown Fixed Identity Networks*", 24th Proceedings of annual ACM symposium on distributed computing***,** 2005.
[14] M.BalaGanesh, M.Mohamed Faisal, "Enhance the Security Level of MANET's Using Digital Signature", *IEEE Transactions on Networking*, Aug.2004.
[15] Sureka.N, S. Chandra Sekaran,"Securable Routing and elimination of Adversary Attack from Manet", proceedings of ICGICT'14, Mar.2014
[16] Tarun Kumar Mishra, Bhupendra Singh, ArunKumar,"A Security Scheme for Mobile Ad-hoc Network with Reduced Routing Overhead ", International journal of advanced research computer science and software engineering, 2013.
[17] MarcinPoturalski, PanosPapadimitratos, Jean-Pierre Hubaux,"Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility", Proceedings of ASIACCS, 2008.
[18] Sharon Goldberg, David Xiao, EranTromer, Boaz Barak, Jennifer Rexford,"Path-Quality Monitoring in the Presence of Adversaries", Proceedings of ASIACCS, 2008.
[19] Amitabh Saxena and Ben Soh,"One-Way Signature Chaining - A New Paradigm For GroupCryptosystems", International Journal of Information and computer Security, 2006.
[20] Prosenjit Bose and Pat Morin and Ivan Stojmenovi´C and Jorge Urrutia,"Routing with Guaranteed Delivery in Ad Hoc Wireless Networks", Journal Wireless Networks vol 7 Issue 6, Nov 2001.

BIOGRAPHIES

Ms. M.Mohana is doing her Master of Engineering in Computer Science & Engineering at Sri Vidya College of Engineering & Technology, Virudhunagar. She completed her Bachelor of Technology in Information Technology at Nandha Engineering College, Erode. Her area of interest is Wireless Sensor Networks.

Ms.P.Kaviya is working as an assistant professor in Sri Vidya College of Engineering and Technology, Virudhunagar. She completed her Master of Technology in Network Engineering at Kalasalingam University, Krishnankoil. She completed her Bachelor of Engineering in Computer Science & Engineering at Kamaraj College of Engineering & Technology, Virudhunagar. Her area of interest is Wireless Sensor Networks.