International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey of Prevention Techniques for Denial Service Attacks (DoS) in Wireless Sensor Network

Jitendra R. Patil[1], Manish Sharma[2]

[1]M.Tech. Student, Department of Computer Science & Engineering, SVCE, Indore, Madhya Pradesh, India

[2] Guide & Assistant Professor, Department of Computer Science & Engineering, SVCE, Indore, Madhya Pradesh, India

Abstract: ***Wireless sensors are very small embedded devices with low memory, low computing power and low battery life. Various applications such as continuous connectivity, weather monitoring, industry and instantly -deployable communication for first responders and armed. These networks already consider environmental conditions, factory performance, and troop deployment, to name some applications. Wireless ad-hoc sensor network is gaining popularity in all organization and it is basic means for communication. Wireless ad-hoc sensor network is defenseless to Denial of Service (DOS) attack. DOS attack create the network resources is absent to users. In DOS attack it creates the node to consume more battery power and reduces the network performance. Different techniques are used for detection and avoidance of DOS attack such as packet leash, lightweight Secure Mechanism, spread spectrum and energy weight monitoring scheme (EMWA) but DOS attack cannot fully legitimate using this techniques. This paper survey of various types of DOS attacks and its Detection and Prevention methods.***

Keywords: Network Security, DoS attacks, Vampire Attack, EMWA

1. Introduction

Wireless sensor network is the second category. Wireless sensor network were firstly designed to facilitate armed operations but today it's used for monitoring and recording the physical conditions of the atmosphere and organizing, such as health, Humidity, wind speed and direction, traffic and other industrial areas. Nodes in Wireless sensor networks are connected to each other and forms the networks. The sensor nodes in the wireless sensor networks are typically dependent on the battery power. To saving the power of nodes may be used a number of techniques. In the some reason of energy loss in wireless sensor network node in the idle depletion, when the nodes are not contributing in the processing of transmitting or receiving any information but listening and waiting for information from other nodes.

By networking large numbers of tiny sensor nodes, it is possible to obtain data about physical occurrences that was difficult or not possible to obtain in more conventional ways. In the coming years, as developments in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, growing deployments of wireless sensor networks are projected, with the networks eventually growing to large numbers of nodes. After the initial deployment (typically ad hoc), sensor nodes are responsible for self-organizing a proper network arrangement, often with multi-hop connections between sensor nodes. The onboard sensors then start collecting audio, seismic, infrared or magnetic information about the environment, using either uninterrupted or event driven working modes. In the location and positioning information can also be obtained over the global positioning system or local positioning system. This information can be gathered from across the network and appropriately processed to construct a global view of the monitoring occurrences or objects. The basic thinking behind wireless sensor networks is that, while the ability of each separate sensor node is limited, the collective power of the entire network is enough for the required task.

2. DoS Attacks on Sensor Networks

Wireless Sensor networks are defenseless to security attacks due to the broadcast environment of the transmission medium. Furthermore, wireless sensor networks have an extra vulnerability because nodes are often placed in an inauspicious or dangerous environment where they are not physically protected. Basically attacks on sensor network are categorized on to two type i.e. active attacks and passive attacks.

DoS attack is active type of attack. Denial of Service (DoS) is a widespread threat in today's networks because DoS attacks are easy to launch, while protecting a network resource against them is suspiciously difficult. Despite the extensive research in recent years, DoS attacks continue to damage, as the attackers get used to the newer protection mechanisms. For this purpose, we start our study with a historic timeline of DoS incidents, where we illustrate the variety of categories, goals and motives for such attacks and in what way they evolved for the duration of the last two decades. We then provide an extensive literature survey on the existing research on denial of service guard with an importance on the research of the last years and the most demanding aspects of defense. These include traceback, detection, taxonomy of incoming traffic, reaction in the presence of an attack, mathematical modelling of attack and protection mechanisms. There are many categories of Denial of service attack discuss as follows:

1) Denial of Sleep Attack

In wireless sensor network denial of sleep attack is one of type of DOS attack. This kind of attack is firstly mention by stanjano and anderson in 2000 as sleep deprivation torture. The sensor power supply is mainly targeted in effort to

exhaust this constrained resource which has devastative impact on the network life time.

2) Warmhole Attack

In a wormhole attack, challengers cooperate to give a low-latency side-channel for communication. For example, two attackers may have a second radio for communicating over a higher-power, long-range link.

Messages received at one attacker are transmitted to the other using the side-channel, where they are transmitted as if only one-hop away from the source [1]. This ability to define ones distance from another node may cause neighbouring nodes to favour the attacker for routing another example of a sinkhole. As long as the side-channel exists, service may actually be enhanced, instead of denied. However, when the attacker moves or ceases to tunnel messages, the network may be left in an inconsistent state that requires re-initialization of some

3) Jamming

Jamming attack is the type of Denial of Service attack. The jamming attack are two types such as Jamming under the external threat model of jamming and internal threat model of jamming. In the external threat model in jamming is not the part of network and jamming attack is transmits the high power nosiness signal continually or randomly. In internal threat model any knowledgeable adversary who is aware of network secrets and operations details of protocol of the network beginning selective jamming attack [2]. In selective jammer attack message with high importance are targeted.

4) Path Based DOS Attack

This attack is exist in special network structure required the sensor network is the two level hierarchical structure with the cluster head nodes and the nodes in cluster at the same time the network has also dedicated path nodes to a main form of attack target at physical layer in wireless sensor network.

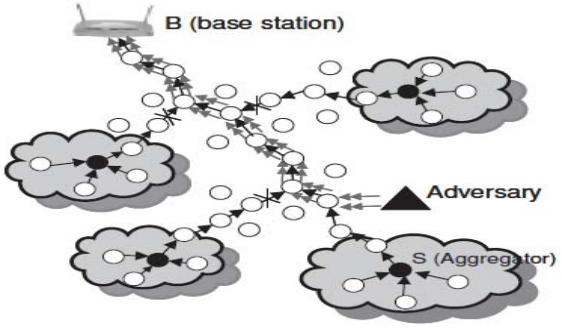

Figure 1: Path Based DOS Attack

5) Vampire Attack

Denial of service (DOS) attack is a try to create a machine or network resource absent to its intended users. In power consumed opponent is attacks on the node and depletion extra battery power of the node [3]. Vampire attack is one of the type of power consumed attack .In carousel attack opponent sends the packet in routing loop and in the stretch attack infected node sends the packet in longest possible route so that it consumes extra battery power of the node. In vampire attack node is depletion extra battery power for its packet transmission. If the node consumes more battery power then it can be discharge and disconnected from rest of the networks. Vampire attack forms by the combination of carousal attack and stretch attack. These two attacks mainly focus on decreasing the energy of the nodes.

a. Carousal Attack:

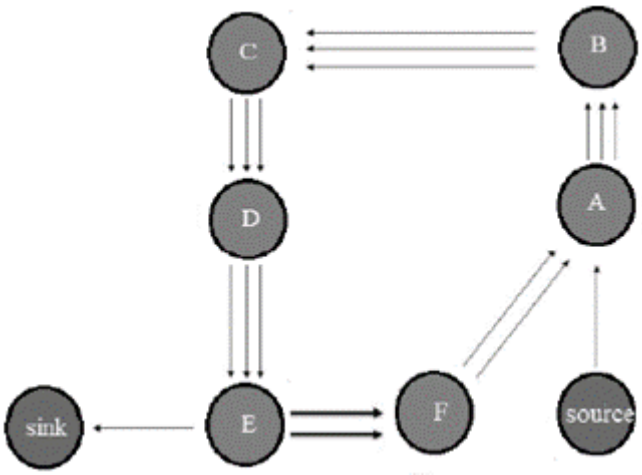

Figure 2: Carousel Attack

In Carousel attacks, opponent node forward the packets in routing loop as shown in fig 2. In fig 2 of the carousal attack, packet is forward from source to sink. If we forward the packet from source to sink then shortest route is from source to node F to node E to Sink. But here packet is not monitors the shortest route. Opponent attacks on the network and forms the loop as shown in figure 2 Packet is send from source to node A. The node A forward packet to next node B. Then node B sends packet to next node C. Node C forward packet to node D. Then node D forward packet to node E. Then node E instead of sending packet to Sink, it is forward packet to node F. Then the node F forward packet to the next node A and create loops. Then same path is repeated again and again many times and it effects extra energy used up by the nodes in that situation the energy depletion of the wireless sensor network performance is reduces.

b. Stretch Attack

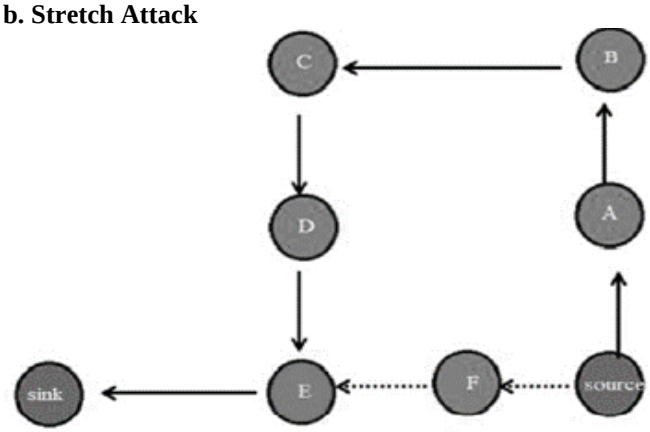

Figure 3: Stretch attack

In Stretch attack, an opponent constructs artificially long routes and potentially pass through every node in the network. In these attack it increases path length of the packet. In fig 3 packet sending from source to sink. The shortest path for forwarding packet is source to node F to node E to sink but here in Stretch attack, an adversary forward packet in

longest path as shown by dark line in fig 3 so it increases energy usage by the network. As carousel attack is depending on position of attackers, Stretch attack is more effective and this attack is independent on attacker's position relative to the destination.

3. Detection Techniques

1. Detection techniques of Denial of sleep attack

In Denial of sleep attack describes the host based lightweight intrusion detection technique, Clustered Adaptive Rate Limiting based on the rate limiting approach at MAC layer is proposed to prevent denial of sleep attacks. The primary shortcoming of above technique is that the period during which nodes are awake is not synchronized, so if a node has packet to send, there is no guarantee that other nodes will poll at proper time to overhear a portion of preamble and remain awake for the data packet. The technique used in B-MAC increases latency in multi hop networks and if bursts of network traffic are generated at a higher rate than is supported by rate-limiting policy, network traffic is lost. So in adaptive rate limiting, network traffic is prohibited only when malicious packets have been sensed at a rate sufficient to suspect the attack. That technique can be used to maintain network lifetimes and better throughput at a time even in face of sleep deprivation attack.

2. Detection techniques of Warmhole Attack

Packet leash [4] is a techniques for detecting and thus preventing against wormhole attacks. A leash is any information on that is inserted to a packet designed to restrict the packet's maximum allowed transmission distance. This techniques uses two types of leashes for this purpose: Geographic and Temporal. In Geographic Leashes, each node knows its precise position and all nodes must have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, calculate the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to detect whether the received packet passed through wormhole or not. In Temporal Leashes, the sender appends the sending time to the packet and the receiving node calculate a travelling distance of that packet assuming propagation at the speed of the light and using the difference between packet sending time and packet receiving time. This solution requires a fine-grained synchronization among all nodes

3. Detection techniques of Jamming

In jamming attack adversary attack in the network under external and internal threat model. In the external threat model jammer is not part of the network. In external model jammer is continuously or randomly transmits high power interference signals. For the prevention of jamming attack from external jammer spread-spectrum communications technique used. Spread Spectrum techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. In the jamming under internal thread model any sophisticated adversary who is knowledge of network protocol can launch selective jamming attack. To launch selective jamming attack adversary must be capable of implementing "classify then jam" strategy before completion of wireless transmission. After classification, the adversary must introduce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. For the prevention of jamming attack from internal thread model use packet hiding method. In packet hiding method before classification of the packet by adversary we hide the packets. Hence adversary can't add bit error in to the packet and it is securely transmits. For the packet hiding method use commitment methods and cryptographic puzzle. In commitment method sender commits the packet and it is verify by the verifier. In the cryptographic puzzle packet m is encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

4. Detection techniques of Path Based DOS Attack

In this path based DOS attack is launched by flooding data packet along multi hop end to end path. To defend against path based DOS attack an intermediate node must able to detect spurious packet or replayed packet and then reject them. For the detection of spurious packet use lightweight secure mechanism to defend against path based DOS attack. In this mechanism configures one way hash chain along a path enabling each intermediate node to detect a Path based DOS attack and prevent propagation of spurious or replayed packet. Every packet sent by end point includes new one way hash chain number which is used for message authentication. Different hash chain number is used for each time slot and intermediate node forward packet only if new hash chain number is verified. This process of verification by each intermediate node is continue and each time slot it verify new hash chain number. If number is not validate then the drop the packet.

5. Detection techniques of Vampire Attack

The mechanism of preventing vampire by using energy weight monitoring algorithm(EWMA).In this algorithm energy of the node is consider for find out threshold level of the node. Find out malicious node in the network every node is add the test field while receiving the packet and forward packet to next node. Then test field is check for each node. if the test field is correct then normal operation is continue and if the test field is wrong then create an alarm packet. Then alarm packet is broadcast and announce that node is malicious so that it avoid for further communication. That malicious node reaches its threshold level. This algorithm is divided in two phases such as communication phase and network configuring phase.

In network configuring phase establish optimum routing path from source to destination. Attacked node consumes more energy and reaches threshold energy level. In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After

receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node upon receiving this stored in its routing table to facilitate further computations. Now the node is establishes the routing path from source to destination. The source nodes select the node which is less distance from source and require minimum energy to transmit the packet.

In communication phase avoid same data packet transmitted repeatedly through same node. These repeatedly transmission of same packet through same node depletes more battery power of the node and degrade the network performance. The process of repeating the packet is eliminated by aggregating the data transmitting within forwarding node. In data aggregation copy the content of the packet which is transmitting through the node. This copied content compare with the data packet transmitting through the node. If the transmitted packet is same as the copied packet then stop the packet transmitted through them. In this way it avoids the redundant packet transmitting through the same node and protect from the vampire attack.

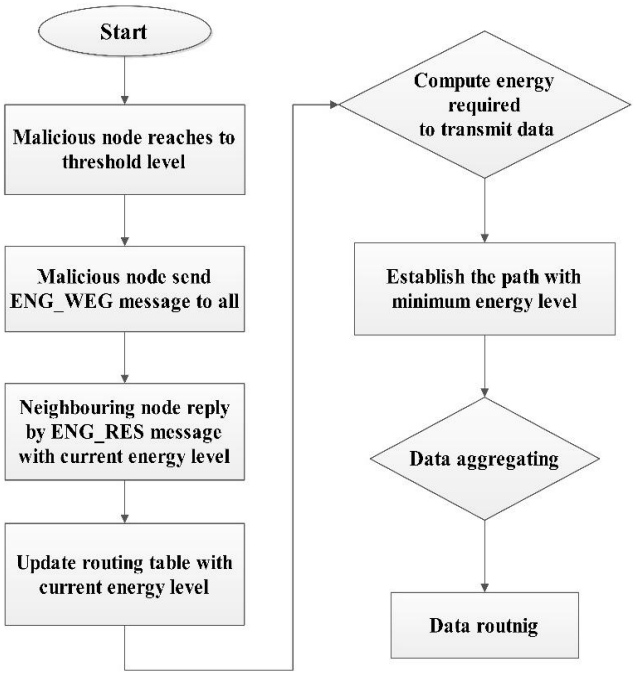

Figure 4: Energy Weight Monitoring algorithm (EWMA)

4. Discussion

Type of DOS attack	*Detection technique*	*Features*	*Disadvantages*
Denial of Sleep	lightweight intrusion detection technique	Clustered Adaptive Rate Limiting based on the rate limiting approach at MAC layer is proposed to prevent denial of sleep attacks	It consider attacks only at the Medium Access Control (MAC)
Wormhole Attack	Packet Leash	Allow connection between two non-neighboring malicious node	Solution Comes at high cost and not always applicable
Jamming Attack	Spread Spectrum	Archiving strong security and prevention	Spread Spectrum fails against
	and Cryptographic puzzle	of network performance degradation	internal threat model
Path Based DOS	Lightweight Secure Mechanism	Adversary cannot generate valid OHC number	It tolerate the packet losses
Vampire Attack	Energy Weight Monitoring System	It avoid redundant packet transmission or loop and saves power of the nodes	Not offered fully solution for vampire attack during topology discovery phase

5. Conclusion

DOS attacks is easier to launch in ad-hoc wireless sensor network. In this paper described the different type of Denial of service attacks such as Jamming, path based DOS attack, power consumption that permanently disables the ad-hoc wireless sensor network. Our aim is to study the various kind of denial of service attack and its prevention techniques. After developing the many prevention techniques wireless ad-hoc sensor network still unsafe to denial of service attacks. Denial of service attacks is critical problem for users. In the future we improve our techniques for prevention of denial of service attacks which are not yet able to prevent denial of service attack fully.

6. Future Scope

In this paper, we done survey study and analysis of various vampire attack detection techniques but techniques have some pros and cons, there is need to develop a such technique, that overcome all these disadvantages with a proper vampire attack and prevention also so that Network will more secure form miss users.

References

[1] Anthony D. Wood and John A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks” Department of Computer Science University of Virginia fwood.
[2] Alejandro Proan˜o and Loukas Lazos, “Packet hiding methods for preventing selective jamming attack”, IEEE Transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012.
[3] Eugene Y. Vassermann and Nicholas Hopper “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks” IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.
[4] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 “Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks”, Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications, pp. 267- 279.
[5] Anthony D. Wood and John A. Stankovic, “Denial of service in sensor networks”, Computer 35 (2002), no. 10.
[6] David R. Raymond and Scott F. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defences”, IEEE Pervasive Computing 7 (2008), no. 1.

[7] Raymond D. R., Marchany R. C., Brownfield M. I., Midkiff S. F., "Effects of Denial-of Sleep Attacks on Wireless Sensor Network MAC Protocols", IEEE Transactions on Vehicular Technology, Vol. 58, Issue 1, pp. 367-380, January 2009.
[8] Jing Deng, Richard Han, and Shivakant Mishra "Defending against Pathbased DoS Attacks in Wireless Sensor Networks" ACM workshop on security of ad hoc and sensor networks, 2005.
[9] A. Wood and J. Stankovic. Denial of Service in sensor networks. IEEE Computer, pages 54-62, Oct, 2002.
[10] Sharnee Kaul, Helen Samuel, Jose Anand3 Defending Against Vampire Attacks in Wireless Sensor Networks, International Journal of Communication Engineering Applications, Vol 05, Article C084; March 2014
[11] Jyoti Thalor, Ms. 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
[12] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
[13] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.
[14] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

Author Profile

Jitendra R. Patil, M. Tech student in Swami Vivekanand College of Engineering, Indore affiliated to Rajiv Gandhi Technical University, Bhopal (M.P) and completed the B.E degree with stream of Information Technology, in 2010 from R. C. Patel Institute of Technology, Shirpur, affiliated to North Maharashtra University, Jalgoan (M.S). Life member of IAENG, IACSIT and CSTA. Research interest includes Network Security, Wireless Networking and NS2.

Manish Sharma, Reader Department of Computer Science & Engineering at Swami Vivekanand College of Engineering, Indore affiliated to Rajiv Gandhi Technical University, Bhopal (M.P), Received BE From Jawaharlal Institute Technology (JIT) Borawan (Khargone) in 2009.He also received M.Tech from Acropolis Institute of Technology and Research (AITR), Indore in 2014. He published various Papers in International and National Journals. His specialization in Computer Network, Theory of Computation. His Research Area is Information Retrieval and Genetic Algorithm.