International Journal of Soft Computing 11 (3): 221-226, 2016
ISSN: 1816-9503

A Detailed Survey on Security Attacks on Wireless Sensor Network and its Countermeasures

P. Sherubha and M. Mohana Priya
Department of Computer Science and Engineering,
Karpagam University, Coimbatore, Tamil Nadu, India

Abstract: Wireless Sensor Networks (WSN) is tranquil of small, stumpy cost, resource-constrained computing nodes set with low power wireless transceivers. Their unattended nature and possible exploitation in antagonistic environmental conditions poses several confronts in ensuring that a WSN is formed effectively and continue to exist long enough to accomplish its function. Therefore, WSN networks have their individual vulnerabilities that cannot be always undertake by these wired network security solutions. Denial of Service (DoS) attacks has also become a crisis for users of computer systems associated to the Internet. In order to thwart Denial of Service (DoS) attacks in WSNs, present study initiated methods to get rid of DoS attacks approach. We show its efficiency in various attack scenarios, discuss motivation for its operation. Our primary purpose for this research is to kindle the research community into developing original, effectual, efficient and complete prevention, discovery and response mechanisms that address the DoS flooding difficulty before, during and after a definite attack. Detailed examination on all these constraint using different methodology was made in this work to reveal the efficiency and heftiness of the internet resources.

Key words: Denial of service, flooding, resource constraint nodes, heftiness, WSN networks

INTRODUCTION

Wireless Sensor Networks (WSN) are self-possessed of low cost, low power, undersized computing nodes, communicating by wireless to observe and/or manage some aspects of the situation in which they are entrenched. Due to their broadcast communication, restricted resources, unattended character and antagonistic environmental conditions, there are many confront to guarantee the protected and consistent operation of a WSN. Like any supplementary communication network, WSNs are vulnerable to intrusion and attacks by spiteful entities. The intention of such entities is to disrupt or cripple the process of a WSN, by negotiation of individual sensor nodes in the WSN. Many Denial of Services (DoS) attacks have been worked out by researchers. These DoS attacks nonetheless are not defined in a succinct manner. Researchers have different description for same attacks and sometimes same descriptions are used for multiple attacks. There are numerous types of attacks that sensor nodes are susceptible to such as Blackhole, Wormhole, Sybil, Replay, modification, Hello-flood which is the spotlight of this study.

Initial contribution of this work is to guarantee the network nodes that forwarded packets are free from Denial of Service attacks (DoS) in which it causes data to loop in the network. Secondly, several countermeasures are taken to improve the routing infrastructure to avoid the vulnerabilities in the network resources (Gracelin *et al*., 2010). In this study, survey on DoS attacks and its countermeasures are updated, to demonstrate the works of the researchers.

MATERIALS AND METHODS

Description of attacks

Black Hole (BH) attack: In a black hole attack, a spiteful node joins the network and then either throw-out all the messages it receives or execute selective forwarding. The roguish node waits for the neighbor to commence a RREQ packet. As the node receives the request, it straight away sends a false reply packet with higher sequence number (Sangi *et al*., 2009). So, the source node considers that the node is having fresh route towards destination. Hence, the source node starts sending the packets over spiteful node (Jeni *et al*., 2013). It doesn't allow forwarding of packets thus swallows the data packets. Analysis of

Corresponding Author: P.Sherubha, Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamil Nadu, India

TSDRP under black hole attack (Chaubey *et al*., 2015) provides better performance parameters such as Packet Delivery Function (PDF), Average End to End Delay (AED) and Average Throughput (AT), Normalized Routing Load (NRL).

Flood rushing attack: Being route detection as an objective, the adversary node tries to send route request to the source node. The first route request is being acknowledged and the remaining requests (flood suppression) are being discarded (Yi *et al*., 2005). Thus, an adversary node rouges the route discovery request without any specified delay (Xiao *et al*., 2008). Thus, it leads to a network-load by imposing false Route Request (RREQ). Processing time of such nodes increases overhead. Exhaustion of nodes battery power in order to measure the impacts of flooding attack, the AODV routing protocol is presented (Sangi *et al*., 2009). It includes route maintenance mechanism to notify periodic beacons of the neighbor links for detecting and monitoring of false request.

Wormhole attacks: In a wormhole attack, an attacker accounts packets (or bits) at one location in the network, channels them to another location and retransmits these into the network. A wormhole attack not only hold back correct routing but is also the precursor to many other attacks such as black hole, sink hole, etc. In a wormhole attack the channel is usually a low latency link. However, wormhole is channel spanned over multiple hops and we suppose that the delay in propagation depends on the number of hops a message has traveled, thus making the wormhole channels a low latency link. Perhaps, the requirements can be improved by defining a Hop Count metric and by considering that the two genuine nodes at the end of the channel are more than four hops away (Hop Count>4) (Mukkamala and Sung, 2003). The assaults include the operation of two or more adversarial nodes. Hoping count will be increment when the packets are forwarded along the routes of the network. The main objective of wormhole attack is to reduce the hop counting (Sangi *et al*., 2009), thus making probability of choosing the adversary nodes is higher.

Secured routing protocol has higher effect on routing directions and selection of Route Request (RREQ) to eliminate adversary nodes.

Gray hole attack: Grey hole exist in stand alone or cooperative versions. The malicious nodes have higher reputation and behave well around vicinity. Misbehaving nodes turned up with certain timing. It is an expensive task in terms of message overheads and communication speed (Chaubey *et al*., 2015). LEACH routing protocol provides better performance in terms of metrics like packet drop ratio, throughput and Average End to End delay (Tarman *et al*., 2001).

Modification attacks: The introduction of spiteful node in the network alters the destination address in the topology by preventing the routing packets not to arrive at the intended destination. Malicious node Detection and Elimination (MDE) (Saghar *et al*., 2016) is a novel approach to sense and get rid of the malicious node in the topology. When the node receives the beacon for the first time, it will compare with its other beacon signals received from its neighbors and ensures the node for changes in the destination address of the packet received. The node will update their neighbor tables by receiving the beacon packets, from its neighbor. Thereby eliminating the malicious node in the network.

Spoofing attack: A spoofing attack is the procedure of changing or repeating routing information (data, beacon or acknowledgement packets). It can lead to the formation of imprecise or unbalanced routes. A spoofing attack can be defined as direct spoofing, in which an assailant node, upon receiving a message, changes the stuffing of the message before retransmitting it or indirect spoofing in which an assailant, node upon eavesdropping a message, sends it to another node by altering the message. In a direct spoofing assault the attacker, upon receiving a message, either retransmits it with a counterfeit sender or modifies its data. Note that the destination is not significant here rather, the node ID to which the message is forwarded is more significant.

Sybil attack: A sybil attack happens when a malicious node zin attendances manifold identities concurrently within the network. Such a node may be used to challenge the routing protocols that rely on redundancy (Saghar *et al*., 2016) such as multi-path protocols. The specifications of a sybil attack states that a spiteful neighbor, Natk (node neighbor attack) uses a set of fictitious IDs, FalseId as a substitute of using its original node ID as message sender in the message transmission. The fictitious IDs must be an ID of a node present in the network. How the attacker gets these IDs is not significant here.

Hello-flood attack: A hello flood assault engages the use of a high power transmitter by an attacker to transmit routing or other information with the idea of persuasive every node within the radio range that the attacker is a rightful neighbor (Saghar *et al*., 2016). The attacker may

then be recognized in routes that are not viable by other nodes since their transmitters are much less influential. The stipulation state that attacker node Natk has a number of nodes within its radio range from the network explains as all nodes. Note that these links are unidirectional (InRange), e.g., Natk can be a processor class or an influential transmission node, i.e., can transmit the message with large transmission power. Only a number of the nodes, some nodes have this attacker node within its radio range as well (Papadimitratos and Haas, 2002). The residual nodes do not have Natk in their radio range and the present node Ncur (current node) is part of that group. Therefore, on every occasion an attacker node transmits, it is heard by all nodes and thus could induce most nodes in the network that Natk is their neighbor (Li *et al*., 2006).

Sinkhole attack: In a sinkhole attack, a spiteful node, Natk, draws all the adjacent traffic by making itself striking to all nodes within the radio range (Fraser *et al*., 2007). This assault is possible if Natk with a long range can offers nodes within the radio range a smaller hop path (hello flood), maintain that Natk is the base station itself (or near to the base station) by a spoofing attack or offers a shorter/faster hop path using wormhole/INA. After adding up itself to the network by flattering attractive the attacker opens a black hole attack and thus plunges data packets (Dey *et al*., 2008).

Jamming attack: Jamming is a physical layer assault initiated by generating radio noise in an exacting physical area (Saghar *et al*., 2016). The stipulation for a jamming attack state that there is a spiteful neighbor, Natk, within its radio range. When Ncur transmits messages some of its neighbors (some neighbors) receive this transmission but the remaining adjacent nodes do not obtain due to the RF noise formed by Natk. Note that the receiving neighbors might be unacceptable as stated by the stipulation. Thus, jamming can avoid a few or all neighbors to obtain the messages transmitted by the node Ncur.

Node replication attack: A node duplication attack is similar to a sybil attack excluding that the attacker uses the same identity (SameId) for numerous nodes. Thus, a single opponent node may signify many practical locations in the network (Dasgupta *et al*., 2009). These multiple nodes must be spiteful Nodes because these are either the attackers or cooperation nodes. All these spiteful nodes have an ordinary ID, i.e., SameId. One of these spiteful nodes, Natk, deceit within the radio range of the current node Ncur. Thus whenever Natk broadcast a message, the sender ID is constantly the ID, SameId.

False-injection attack: A false injection attack refers to the foreword of additional data or organizes packets into the network. It devours bandwidth and may source routing loops. The main intention of this attack is to devour resources extravagantly (Saghar *et al*. 2016). In our description of a false injection attack a spiteful neighbor Natk of rightful node Ncur, introduces additional message packets into a network. Unlike the spoofing attack, the message introduced might not be the similar as the one received earlier (Mr) or some counterfeit message, Mf. Therefore, the main aspire here is to insert additional traffic. It is also dissimilar from INA as the attacker may insert the messages many times (Fu *et al*., 2008).

Invisible Node Attack (INA): Researchers describe the wormhole attack in two diverse ways. One description employs the out of bound channel, where two attacker nodes are required. Some dispute that the wormhole is even possible with a solitary attacker's node using the packet communication. But the packet relay is also defined as an Invisible Node Attack (Saghar *et al*., 2016) (INA) by many researchers and we also extravagance it as a diverse type of attack from wormhole attack in which the attackers range is different, more overwhelming and the use of concealed channel means the attackers stay behind undetected (Adaobi *et al*., 2012). On the other hand, in INA the radio range is inadequate by the attacker's potential and because it uses the same channel and the nodes also notice the same message impending back to them. Note that in the stipulation of INA, the same attacker is a neighbor of both the rightful nodes (Shea and Liu, 2013). This makes the stipulation of INA quite alike to a wormhole attack in an intelligence that there is one spiteful node which is a neighbor of both unconnected rightful nodes and the rightful nodes can take delivery of the same message back when an attack is initiated (Renold *et al*., 2012).

RESULTS AND DISCUSSION

DoS attacks elimination methods- overview: An overview of DoS attacks is presented in this section. It provides an amount of information regarding the different forms of denial of service attacks (Almomani and Al-Kasasbeh, 2015).

Ingress filtering: For the past several years DoS attacks are fertile area of research. One way to address the problem of DoS attacks is to eliminate the ability to forge source addresses. One such approach is known as ingress filtering to configure routers to block packets that arrive illegitimate source addresses (Fu and Papatriantafilou, 2012). The principal problem is that its

effectiveness depends on significant fractions of ISPs. It is clear that the wider use of ingress filtering would improve the internet's robustness to denial of service attacks (Rotenberg *et al*., 2014).

Link testing: One of the most existing trace back techniques, router closest to the victim and appropriately test its upstream links until they determine which is used to carry the attacker's traffic. This technique assumes that an attack remains active until the completion of the trace (Antikainen *et al*., 2014). This link testing describes two schemes towards Dos attacks.

Input debugging: Most routers allow input debugging, that allows an operator to filter particular packets and to determine which ingress port they arrive on. There are certain methods to implement trace back as follows: Initially the victim must recognize that it is being attacked and develop an attack signature that describes a common feature contained in all attack packets. The victim communicates this signature (Song and Perrig, 2001) to the network operator via telephone, who then installs a corresponding input debugging filter on the victim's upstream port. This process is repeated recursively until the originating site reached and traced back (Savage *et al*., 2000). The most obvious problem with the input debugging approach is its considerable management overhead. Communicating and coordinating with network operators at multiple ISPs requires time, attention and commitment of both the victim and the remote personal (Admas and Lloyd, 1997). If the appropriate network operators are not available or if they are unwilling to assist, then a trace back may be slow or impossible to complete (Fu *et al*., 2012).

Controlled flooding: A link testing trace back techniques that does not require any support from network operators, hence called as controlled flooding technique. It tests links by flooding them with large bursts of traffic and observing how it perturbs traffic from the attackers (Bandyopadhyay *et al*., 2011). Using a pre-generated map of internet topology, the victim forces selected hosts along the upstream route into iteratively flooding each incoming link of the router closest to the victim. Since, the router buffers are shared, packets travel across the loaded link-including the packets sent by the attackers have an increased probability of being dropped (Carzaniga *et al*., 2004). By observing this packet flow, the rate of packets received from the attackers, the victim can therefore infer which link they arrived from.

Most problematic among these is that controlled flooding is itself a denial-of-service attack exploiting vulnerabilities in unsuspecting host to achieve its end. This drawback itself makes it unsuitable for routine use (Phulre *et al*., 2014). Also, it is unsuited for distributed denial of service attacks.

Logging: This approach is to log packets at key routers and then use data mining techniques to determine the path that the packets traversed (Song and Perrig, 2001). This method has a useful property that it can trace an attack long after the attack has completed. However, it has drawbacks, including enormous resource requirements.

ICMP trace back: The principal idea in this scheme is for every router to sample, with low probability, one of the packets it is forwarding and copies the contents in to a special ICMP trace back message including information about the adjacent routers along the path to the destination (Song and Perrig, 2001). During a flooding attack, the victim host can then use these messages to reconstruct a path back to the attacker. However, there are several disadvantages which complicate its use. ICMP traffic is increasingly differentiated from normal traffic (Carzaniga *et al*., 2004). ICMP trace back message relies on an input debugging capability, i.e., ability to associate a packet with the input port and/or MAC address on which it arrived. Finally it requires distributed infrastructure to deal with the problem of attackers sending false ICMP trace back messages (Rogers *et al*., 2003).

By calling Handle RREQ and Retry RREQ Functions: Another way out to thwart Flooding Based DDoS attack is by vocation Handle RREQ and Retry RREQ functions. Flood attack occurs because of instigate various RREQs on a exacting node. Because of various RREQs that node is not capable to grip more RREQ and becomes spiteful node. When this node move towards the path of other nodes does not promote packets and hectic in handling RREQ. In order to thwart network from this attack, we can call these purpose, i.e., Handle RREQ and Retry RREQ. Handle RREQ utility is to help handling various RREQ which arrives on a particular node and alleviate flood attack. Similarly, retry RREQ function attempts to find another pathway for forwarding packets from source to destination, this pathway may be superior from the path which is through spiteful node but we get the path and packets are reached from source to destination. Both of these existing techniques only alleviate the effect of Flooding Based DoS does not stop it completely (Tyagi and Dembla, 2014).

CONCLUSION

Wireless sensor networks have materialized as a hopeful solution for responsive applications involving serious observational and scrutinized operations. In spite of that their numerous benefits, these networks are susceptible to spiteful attacks that may compromise the appropriate operations of the critical applications. Initial consideration of this work is the denial of service attacks that would disrupt the network activities with the adversary nodes and projects the effects of devastating in the network layer. Secondly, the process of filtering the anomalies from the network nodes has been discussed and a trust based mechanisms is given to repel against misbehavior in the network by stirring to enhance cooperation and to improve the performance. In our future work, we will progress our method by introducing other constraint for detecting DoS attacks and considering other preventing security systems in order to guard wireless sensor networks.

REFERENCES

Adaobi, O., E. Igbesoko and M. Ghassemian, 2012. Evaluation of security problems and intrusion detection systems for routing attacks in wireless self-organised networks. Proceedings of the 5th International Conference on New Technologies, Mobility and Security, May 7-10, 2012, Istanbul, Turkey, pp: 1-5.

Admas, C. and S. Lloyd, 1997. Profiles and protocols for the Internet public-key infrastructure. Proceedings of the 6th IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems, October 31-31, 1997, Tunis, Tunisia, pp: 220-224.

Almomani, I. and B. Al-Kasasbeh, 2015. Performance analysis of LEACH protocol under denial of service attacks. Proceedings of the 6th International Conference on Information and Communication Systems, April 7-9, 2015, Amman, Jordan, pp: 292-297.

Antikainen, M., T. Aura and M. Sarela, 2014. Denial-of-service attacks in bloom-filter-based forwarding. IEEE/ACM Trans. Networking, 22: 1463-1476.

Bandyopadhyay, A., S. Vuppala and P. Choudhury, 2011. A simulation analysis of flooding attack in MANET using NS-3. Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, Chennai, India, pp: 1-5.

Carzaniga, A., M.J. Rutherford and A.L. Wolf, 2004. A routing scheme for content-based networking. Proceedings of 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 2, March 7-11, 2004, Hong Kong, China, pp: 918-928.

Chaubey, N., A. Aggarwal, S. Gandhi and K.A. Jani, 2015. Performance analysis of TSDRP and AODV routing protocol under black hole attacks in MANETs by varying network size. Proceedings of the 5th International Conference on Advanced Computing and Communication Technologies, February 21-22, 2015, Rohtak, India, pp: 320-324.

Dasgupta, M., S. Choudhury and N. Chaki, 2009. A secure hypercube based team multicast routing protocois (S-HTMRP). Proceedings of the IEEE International Advance Computing Conference, March 6-7, 2009, Patiala, India, pp: 1265-1269.

Dey, T., M.M.A. Hashem and S.K. Mondal, 2008. On performance analysis of AMBR protocol in mobile ad hoc networks. Proceedings of the International Conference on Computer and Communication Engineering, May 13-15, 2008, Kuala Lumpur, Malaysia, pp: 128-132.

Fraser, N.A., D.J. Kelly, R.A. Raines, R.O. Baldwin and B.E. Mullins, 2007. Using client puzzles to mitigate distributed denial of service attacks in the tor anonymous routing environment. Proceedings of the IEEE International Conference on Communications, June 24-28, 2007, Glasgow, Scotland, pp: 1197-1202.

Fu, Y., X. Wang and S. Li, 2008. Performance comparison and analysis of routing strategies in mobile ad hoc networks. Proceedings of the International Conference on Computer Science and Software Engineering, December 12-14, 2008, Wuhan, Hubei, pp: 505-510.

Fu, Z. and M. Papatriantafilou, 2012. Off the wall: Lightweight distributed filtering to mitigate distributed denial of service attacks. Proceedings of the IEEE 31st Symposium on Reliable Distributed Systems, October 8-11, 2012, Irvine, CA., USA., pp: 207-212.

Fu, Z., M. Papatriantafilou and P. Tsigas, 2012. Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. IEEE Trans. Dependable Secure Comput., 9: 401-413.

Gracelin, S.R., E.N. Edna and S. Radha, 2010. A novel method for multiple attacks in NTP based routing algorithm. Proceedings of the International Conference on Wireless Communication and Sensor Computing, January 2-4, 2010, Chennai, India, pp: 1-6.

Jeni, P.J., A.V. Juliet, R. Parthasarathy and A.M. Bose, 2013. Performance analysis of DOA and AODV routing protocols with black hole attack in MANET. Proceedings of the IEEE International Conference on Smart Structures and Systems, March 28-29, 2013, Chennai, India, pp: 178-182.

Li, Z., B. Zhao, Y. Qu and K. Chen, 2006. An adaptive and distributed STDMA scheme for ad hoc and sensor networks. Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 23-29, 2006, Morne, Mauritius, pp: 121.

Mukkamala, S. and A.H. Sung, 2003. Detecting denial of service attacks using support vector machines. Proceedings the 12th IEEE International Conference on Fuzzy Systems, Volume 2, May 25-28, 2003, St. Louis, MI., USA., pp: 1231-1236.

Papadimitratos, P. and Z.J. Haas, 2002. Securing the Internet routing infrastructure. IEEE Commun. Mag., 10: 60-68.

Phulre, S., P. Gautam and S.K. Mishra, 2014. Implementation of trusted multitier method for intrusion detection in mobile ad hoc networks with DSR algorithm. Proceedings of the IEEE Science and Information Conference (SAI), August 27-29, 2014, London, UK., pp: 666-673.

Renold, A.P., R. Poongothai and R. Parthasarathy, 2012. Performance analysis of LEACH with gray hole attack in wireless sensor networks. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-4.

Rogers, S.A., S.S.B. Moore and C.A. Siller, 2003. Packet sequencing: A layer-2 WAN switching technology for per-flow ideal QoS and secure IP networking. Proceedings of the IEEE Military Communications Conference, Volume 2, October 13-16, 2003, Boston, MA., USA., pp: 954-959.

Rotenberg, E., C. Crespelle and M. Latapy, 2014. Measuring routing tables in the internet. Proceedings of the IEEE Conference on Computer Communications Workshops, April 27-May 2, 2014, Toronto, Canada, pp: 795-800.

Saghar, K., H. Farid and D. Kendal, 2016. Formal specifications OD denial of service attacks in wireless sensor networks. Proceedings of the 13th International Bhurban Conference on Applied Science and Technology, January 12-16, 2016, National Centre for Physics, Islamabad, Pakistan.

Sangi, A.R., J. Liu and L. Zou, 2009. A performance analysis of AODV routing protocol under combined byzantine attacks in MANETs. Proceedings of the International Conference on Computational Intelligence and Software Engineering, December 11-13, 2009, Wuhan, China, pp: 1-56.

Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2000. Practical network support for IP traceback. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, August 28-September 1, 2000, Stockholm, Sweden, pp: 295-306.

Shea, R. and J. Liu, 2013. Performance of virtual machines under networked denial of service attacks: Experiments and analysis. IEEE Syst. J., 7: 335-345.

Song, D.X. and A. Perrig, 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the 20th Annual Joint Conference on IEEE Computer and Communications Societies, April 22-26, 2001, Anchorage, AK., USA., pp: 878-886.

Tarman, T.D., E.L. Witzke, K.C. Bauer, B.R. Kellogg and W.F. Young, 2001. Asynchronous Transfer Mode (ATM) intrusion detection. Proceedings of the Communications for Network-Centric Operations: Creating the Information Force Military Communications Conference, Volume 1, October 28-31, 2001, McLean, VA., pp: 87-91.

Tyagi, P. and D. Dembla, 2014. Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, September 24-27, 2014, Greater Noida, India, pp: 2084-2090.

Xiao, B., W. Chen and Y. He, 2008. An autonomous defense against SYN flooding attacks: Detect and throttle attacks at the victim side independently. J. Parallel Distrib. Comput., 68: 456-470.

Yi, P., Z. Dai, Y. Zhong and S. Zhang, 2005. Resisting flooding attacks in ad hoc networks. Proceedings of the International Conference on Information Technology: Coding and Computing, April 4-6, 2005, Las Vegas, NV., USA., pp: 657-662.