NUST Journal of Engineering Sciences, Vol 9, No 2, 2016, pp 50-59

DOS Attacks on WSN and Their Classifications With Countermeasures - A Survey

Jahanzeb Shahid, Shahzad Saleem, Muhammad Nauman Qureshi
School of Electrical Engineering and Computer Sciences, National University of Science and Technology Islamabad, 44000 Pak
13msccsjshahid@seecs.edu.pk
shahzad.saleem@seecs.edu.pk

Received: 11 September 2016 Accepted: 10 November 2016

Abstract

Wireless Sensor Networks (WSN) is a network of sensors, actuators, mobile and wearable devices that have processing and communication modules to monitor physical and environmental conditions. Currently millions of these type of smart devices serving in many fields like military, environment, and health services. Due to their unique deployment places even in hostile territories WSN are subject to various kinds of attacks. Self configuration, autonomous device addition, network connection and resource limitation are the main features of WSN that makes it highly prone to network attacks. Denial of Service (DoS) attacks which targets the availability of a WSN system is one of the most potent threat to which a WSN must be resilient in order to continue operations. This studies aim to analyze and classify the WSN DoS threats and their countermeasures. Based on the survey we present the best approach to designing a WSN resilient against DoS attacks.

Keywords: Wireless Sensor Networks, Denial of Service, Countermeasures, Classification, OSI Layer Attacks

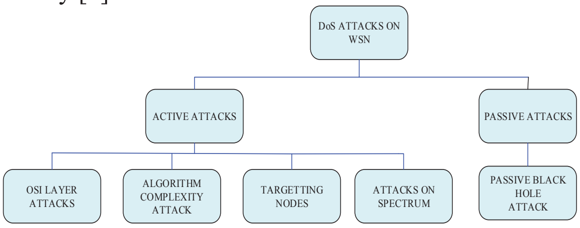
Introduction

A WSN comprises of sensor devices (nodes) that sense or monitor physical and environmental conditions and send this information to each other or to a remote location through co-ordination and co-operation. WSNs have wide applications in different fields such as military and civil surveillance, e-health care systems and climate monitoring. However, with the expansion of the application requirements and fields, sensor nodes often need to be attached to the moving objects, or deployed in the hostile and remote environment, Due to their small size, hostile environment and unattended operations they are highly vulnerable to different security attacks. Limited power resources and low computational power are major constraints for WSN, so defense against security attacks and energy problem is a major concern and a lot of research has been done to overcome these problems. WSNs do not provide much security as wired network, because they suffers from numerous security issues that not only affect their functionality but also their operations.

Generally DoS attacks are large-scaled and coordinated and launched by directing an exceedingly bulk of packets to a target machine. Apart from limited energy, storage capacity and processing, Bandwidth limitation of WSN is also a major issue which raises challenges for the security of WSN. Our contribution in this survey is to classify DoS attacks on WSN in different aspects and providing solutions against these attacks with more details. In section 2 classification of WSN attacks and their countermeasures discussed with details. Future scope is discussed in section 3. Section 4 comprises on conclusion of this paper.

Classificatoin Of Attacks On WSN And Their Countermeasures

In the past DoS attacks were considered as active attacks only [1] but now they can be classified as active and passive. In passive attacks an attacker tries to sniff information from the network but does not try to alter it for example the traditional black hole attack can also act passively [3].



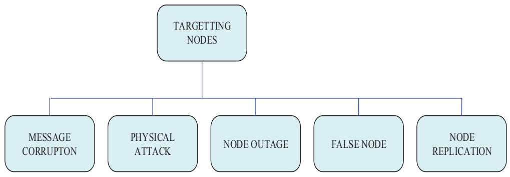
Passive Attacks:

Passive Black Hole Attack: A source node sends data packets but in order to save energy a selfish node drops these packets. So the selfish node is inadvertently paving the way for DoS[4]. Countermeasures for this attack is same as active black hole attack discussed in OSI Layer attacks section.

Active Attacks:

When unauthorized user (intruder or attacker) modifies the data (static or en-route) or alters system resources then it is called Active attack. Now we classify active attacks on WSN.

Node Specific: In this section we discuss DoS attacks that directly affects sensor nodes in WSN.



a. Message Corruption: In this attack, attacker modifies or corrupts data packets on particular node during transmission[5]. Integrity checks on receiver side can drop these corrupted packets, resulting in large number of retransmission requests. In computer security we use hashing to counter message corruption attacks. We cannot use conventional hashing schemes on wireless sensor nodes due to limited computational resources so lightweight hashing scheme are used. Enhanced version of DSDV (Destination Sequenced Distance Vector) protocol which uses simple MD5 hash technique with Merkle hash tree implementation[6] is one example. MACs (Message Authentication Codes) are not resilient to denial of service attack but they can provide en-route message corruption security. Error detection and error correction (EDEC) scheme proposed by Wenbao et al.[7] can guards against message corruption that can lead to DoS attack.

b. Physical Attack: Mostly in WSN sensor nodes are placed in remote and hostile environment and left unattended for a longer period of time, so threat of physical attacks is always associated with these types of devices for example physical tampering, destruction of sensor nodes and corruption of information by tapping other devices with sensor nodes[5]. Mostly WSN might be installed in inhabited area, where physical contact is difficult to make. Sometimes sensor nodes are physically damaged or device's memory probed with special equipment to steal cryptographic keys[2]. To protect against physical tampering and destruction of sensor nodes surveillance and physical monitoring of critical devices might be good solutions. For tapping of devices it is good to use Symmetric key Cryptography for encryption due to low computation of wireless nodes. DiDrip (Distributed Data Discovery and Dissemination) protocol is a proposed scheme for data confidentiality between wireless nodes[8]. It is an energy efficient technique and difficult to crack.

c. Node Outage: is a situation where a node goes down. It may become critical when victim node is behaving as a master node in the network[5]. This attack works when a node gets compromised with intentions to make it out of service. Strong Authentication schemes like Elliptic Curve Cryptography and Identity Based Cryptography can counter this problem. A proposed scheme based on Symmetric-key authentication which is built upon multi-level micro-tesla protocol, staggered-authentication and the Bloom Filter can also be considered [9].

d. False Node: When an adversary introduces some extra nodes into the network with the intentions of poisoning the network then it is called False Node attack[5]. It can further helps in various attacks on network like corrupting routing tables, creating sink hole, jamming or behaving as a false cluster node. This attack should be checked in the routing layer itself. Secure routing protocols like SAODV (Secure ad-hoc On Demand Distance Vector) [10] and DSR (Dynamic Source Routing) can help in this situation[11].

e. Node Replication: A malicious replicated node is added to the network by stealing legitimate node's ID and other parameters. An attacker can manipulate a part of the network or can do intense damage [5]. In research studies Time-Synchronization based scheme is available as countermeasure for this attack which monitors timing information of each node added to the network, detailed functionality of this scheme is presented in [5]. Moreover there are other recently proposed schemes such as Quorum-Based Multicast and Star-shape Line-Selected Multicast for this attack.

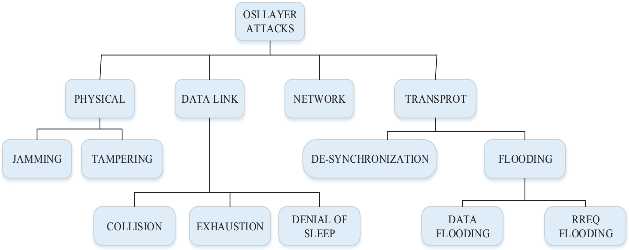
Table1: Attacks Targeting Nodes and their Defenses

Attack	Defenses
Message Corruption	Data Integrity Checks, Hashing, MAC techniques,
Physical Attack	Surveillance, Monitoring, Symmetric Key Cryptography, DiDrip
Node Outage	ECC and Identity based Authentication, Staggered Authentication, Bloom filters
False Node	SAODV, DSR
Node Replication	Time Synchronization, Quorum base multicast and Star Shape Line multicast

OSI Layer Attacks:

Now we classify and discuss DoS attacks w.r.t. different OSI layers and their respective countermeasures [12][13][14].

a. Physical Layer Attacks: Physical layer is mostly endangered by Jamming and Tampering attacks.[12]



i. Jamming Attack: In Jamming attack radio signals of WSN are interfered destructively with radio signals generated by malicious node[2]. The adversary can use one or more nodes to jam the network by transmitting radio signal which interfere with legitimate traffic signals and can block them. Spread Spectrum technique is a well-known solution to these attacks [13] but low computation power of sensor nodes cannot bear this technique. For this frequency hopping spread spectrum (FHSS) scheme suggested in [15] can be used to escape jamming in which data is divided into symbols. These symbols are transmitted continuously by switching radio channels. Jamming identification techniques like PDR (Packet Delivery Ratio), Received Signal Strength Indicator (RSSI) are discussed in [16]. Jammed Region mapping [17] protocol identifies jammed region in WSN but it has problem of overhead in itself. In [14] attacks on different layers and their countermeasures are briefly discussed. Authentication and Security checks with CDMA modulation technique provides defense specially against Jamming attacks.[18] Multi-data flow topologies scheme might be an active defense against mobile jamming attack.[19] Sometimes jammer node may not be a part of network and can jam network communication externally, Packet Hiding algorithm [20] technique is a mishmash of Cryptographic Puzzles that offers protection for jamming. Other Techniques like Priority messages and Lower Duty Cycle provides defensive measures for jamming attacks.[14]

Table 2: Attacks on Physical Layer and Defenses

Attacks	Defenses
Jamming	FHSS, PDR, RSSI, Regional Mapping, Packet Hiding Algorithm, Cryptographic Algorithms
Tampering	Tamper Proof Technique, AODV

ii. Tampering Attack**:** In tampering attack, attacker may damage, replace or electronically manipulate the network to acquire the information that can lead to DoS attack. Hiding sensor devices may save them from physical tampering. Tamper-proofing technique offers defense against message and cryptographic keys tampering [14] but lightweight cryptographic algorithms would give better results in terms of energy efficiency. A tamper-proofing technique is proposed in [21] which is a cost involution based concurrent error detection technique. Packet-Dropping and Message-Tampering prevention can be achieved with AODV (Ad-Hoc On-Demand Distance Vector) enhanced scheme[22].

b. Data Link Layer Attacks:
Collision, Exhaustion, Denial of Sleep lies in the domain of data link layer attacks.

i. Collision Attack: In collision an adversary poisons the frame header that causes checksum mismatch and rejects the data frame at the receiving side[14][13]. Colluding Collision Attack interrupts packets during communication, MCC (Mitigating Colluding Collision) technique which is a modification of BLM (Basic Local Monitoring) offers defense for colluding collision attack [23]. Distributed sampling and centralized analysis of RSSI (Received Signal Strength Index) is proposed by Philip et al.[24]. Error Correcting Code (ECC) is a simple technique to avoid collision.[14]

ii. Exhaustion Attack: Exhaustion attack refers to keeping the channel busy and draining battery life by introducing malicious node in the network, Simple solution is Rate Limitation on each node in network[14]. Fuzzy logic based solution against distributed node Exhaustion attack proposed by Salman et al.[25].

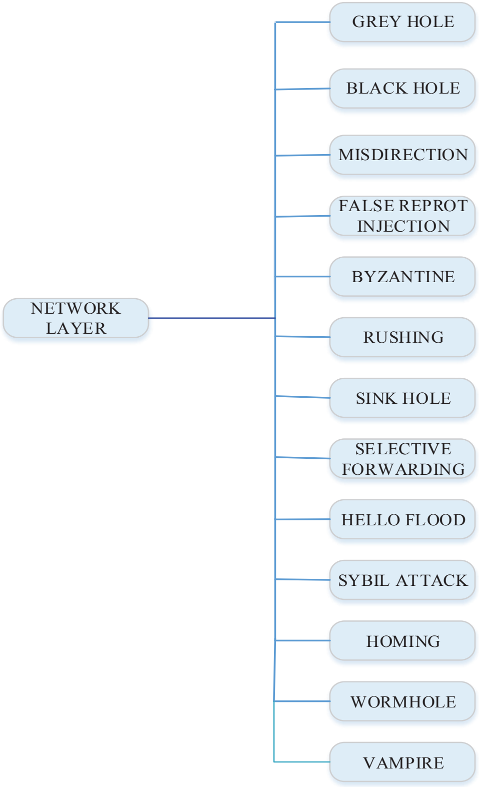
iii. Denial of Sleep Attack: Denial of Sleep attack do not let a node go in to sleep mode and consume power resources by keeping a node up for a long time[26]. Rate limitation based on current host intrusion detection system presents defensive approach against denial of sleep attack[27]. Mitigating techniques like Link Layer Authentication and Anti Replay Protection can be uses for denial of sleep attack[28].

Table 3: Attacks on Data Link Layer and Defenses

Attack	Defenses
Collision	ECC, MCC, CSMA/CA, RSSI
Exhaustion	Rate Limitation, Fuzzy Logic Solution
Denial of Sleep	Link Layer Authentication, Anti Replay Protection

c. Network Layer Attacks: Network layer attacks are also known as routing based attacks. In routing network controller devices help multiple network nodes to communicate with each other. This layer is more vulnerable to number of attacks than any other layer. So we discuss attacks listed in taxonomy diagram one by one.

i. Grey Hole Attack: It is a network layer attack especially in multihop WSN. Sensor nodes sends packets to its neighbor nodes with the confidence that they will forward them to their destination[29] but a malicious node is introduced within the network which rejects packets and ultimately drop the packets instead of transmitting/forwarding them to the next node [30]. If a CH (cluster head) node experiences this attack then it becomes risky for LEACH (Low Energy Aware Cluster Hierarchy) protocol [30] to defend against it. The major difference between grey-hole and sinkhole attacks is that, in sink-hole all the traffic is attracted towards a malicious node and dropped by the node but in grey-hole a malicious node is introduced between nodes and then packets are rejected and dropped, and this malicious node acts like sinkhole between nodes. A distributed intrusion detection system is proposed by Dharini et al. [31] for mitigation at flooding and grey hole attacks. Secure routing algorithm based on ECC (Elliptic Curve Cryptography) for detection of false reports and gray hole attacks [29], gives support against these attacks. An energy efficient technique discussed in [32] for LEACH helps to detect gray hole and prevents a compromised node to become a cluster head.



ii. Misdirection Attack: Forwarding packets to incorrect paths by modifying incorrect routes or an attacker can misdirect packets to a malicious node [33]. Traffic launched from a victim node can be diverted to launch a DoS attack, if distant traffic divert away from the node then receiver node could denied service. This can be done by amending the path in routing which consists of source-routes in each packet [2]. Egress filtering, Authorization and monitoring of routes are general techniques proposed by O. Xi .et al [14] for misdirection attack. Cluster based intrusion detection and prevention technique is proposed in [34]. Authentication of routing updates and cryptographic integrity checks can mitigate misdirection attacks [2].

iii. False Report Injection: In this type of attack false reports are injected into the network from a malicious node which drains the residual power of node and sends false information to base station[29]. The purpose of this attack is to consume partial amount of energy in nodes. The purpose of adding this attack in our classified list comes from its functionality of wastage of node energy which is already limited for a hostile node. If the node energy resource dies out before its expected time then it is not available anymore and leads to denial of service. To counter this attack, hop by hop authentication mechanism which uses fuzzy logic scheme proposed by Kim et al. [35] can be implemented. Statistical En-Route Filtering is used for detection of false report injection [9].

iv. Wormhole Attack: An adversary captures data packets from one node and save them to retransmit into the network later from another node[12]. Multiple corrupted nodes connected through high speed data buses[36] for launching this attack. Flexible routing like Distance Vector protocol can counter wormhole attacks [5]. Challenge bit and its response technique between nodes and packet authentication are other solutions for this attack. Advanced Encryption Standard (AES)-based routing algorithm (so-called AODV-Wormhole Attack Detection Reaction - here referred to as AODV-WADR-AES) is used for securing AODV-based eMANETs against wormhole attacks[37].

v. Byzantine Attack: In this attack an adversary takes control on one or more nodes and force these nodes to work in an agreement and then these nodes behaves illogically [38]. They can perform multiple function like modification of data packets, creating loops in routing policy, dispatching packets on non-legitimate paths and performing selective forwarding which results in disturbance or degradation of the network services [36]. *On-Demand Secure Byzantine Routing protocol* (ODSBR) was formed for this attack [38]. Isolation of compromised nodes with byzantine attack scheme is proposed in [39]. Distributed event detection scheme built on statistical approach endure byzantine attack [40]. Implementation of cluster nodes on FPGA (Field Programmable Gate Array) with byzantine attack secure mechanism is introduced by Stelte et al. [41]. ECDSA (Elliptic Curve Digital Signature Algorithm) based fault tolerant scheme is proposed for large scale WSN [42].

vi. Rushing Attack: It is a new kind of attack that leads to denial of service when used against previous On-demand routing protocols like *Dynamic Source Routing* and Ad hoc *On-demand Distance Vector* and other secure protocol like Ariadne, ARAN and SAODV [36][12]. An adversary accepts a route request packet capture it and deluge the packet rapidly into the entire network before other nodes do their job, when other nodes receive packets then they react. An anomaly detection based IDS proposed by Alheeti et al . [43] used feed-forward neural vector and a support vector machine for intelligent IDS. A solution to secure Dynamic Secure Routing is presented in [44] which is based on Secure Dynamic Source Routing (SDSR) protocol. It is proposed to analyze the outcome of rushing attack on SMT/SRP (Secured Message Transmission)/(Secure Route Reply) protocol. It also evaluates consequence of rushing attack as applicable to SMT/SRP [45].

vii. Sinkhole Attack: This is the most known attack performed by manipulating the routing. An attacker simply forward all the traffic to an attractive node which other nodes consider as shortest hop count path and then drop all data packets to a malicious node [5]. According to Karlof and Wagner [46] in sinkhole attack an adversary tries to pull traffic to a malicious node in network [5]. AODV based secure routing algorithm with mobile agent helps to find malicious node in network [10]. A signature based intrusion detection system used in [47] to find mobile sink node in WSN. For small size WSN sinkhole detection technique proposed for Mintroute protocol [48].

viii. Selective Forwarding: In this attack a malicious node forward only selective packet based on type of packet and reject all other packets coming towards itself .Hop-by-Hop Cooperative detection (HCD) scheme is proposed by Lim et al. [49] to mitigate selective forwarding attacks. A challenge and response based scheme formed in [6] to defend against these attacks. Secure alternative path algorithm in sensor network (SeRINS) technique offers path resilient in case of selective forwarding attack [50] but this technique could not identify malicious node P. Sharma et al [51] proposed number of techniques to defend against selective forwarding attacks.

ix. Hello Flood Attack: In this attack large number of hello packets are sent by malicious node with forged address of base station of from other node and victim node treat these packet coming from legitimate one but quantity of hello packets are kept so high that it overflow victim node memory buffer so it becomes unable to process any other request. This attack become very lethal when uses against network bandwidth. Almost every protocol exchanges HELLO messages in session initiation protocol. In WSN it makes every node to think that attacker node is one hope away in transmission range [2]. Two-way Authentication and Three Way handshake is general solution to mitigate this attack. An efficient Distributed Intrusion Detection System is a well-known defense against

Hello Flood Attacks. Lower Energy Adaptive Cluster Hierarchy (LEACH) [30] [34] algorithm can also be used to mitigate flooding attack. Robust formally Analyzed protocol for wireless sensor networks deployment (RAEED) addresses problem of hello flood attack in wireless sensor networks [52]. A systematic method for stochastic modeling of the challenge-response scenarios in networks that uses slotted carrier sense multiple access with collision avoidance (CSMA/CA) protocols are used against hello flood attack in [53].

x. Sybil Attack: When a node confer itself in forged multiple identities in peer to peer network and disturbs multipath routing and topology of the network, it is named as Sybil attack after a book subject **Sybil** which describes case study of dissociative identity disorder of a woman. To check the identities of suspected nodes a voting-based defense technique allows other nodes to decide suspected nodes legitimate or not. A Centralized Clustering-based hierarchical network scheme is proposed in a research [54] to defend against Sybil Attacks. Location Verification[2] might be another solution for Sybil Attack.

xi. Homing Attack: It is a special kind of attack in which by performing traffic pattern analysis attacker tries to find nodes which have more responsibilities [13]than other nodes such as cluster head nodes or nodes that manage cryptographic key exchanges. One vibrant solution against this attack is strong encryption [14] method. Cryptographic algorithms, message hiding and secure clustering can be used to prevent the homing attack.

xii. Vampire Attack: It is a new kind of DoS attack befalling on network layer and resource depletion (energy or battery drainage) attack [55]. This attack is difficult to detect because it does target multiple network layer protocols like SEAD, Ariadne and SAODV [56]. This attack further classifies into *Carousel attack* and *Stretch attack* [57]. In Carousal attack a packet route is set in such a way that it keeps moving in series loops. In Stretch attack victim node builds a long source path that packets pass through more number of nodes then present in the network. Defense mechanism against vampire attack in forwarding phase is presented by E. Vesserman et al [58]. This is not a fully satisfactory solution but provide some insight for further modification to PLGPa. This approach has also discussed by L. Deshmukh [59] with little modification in PLGPa protocol. But these solution have constraints in terms of nodes memory so an authentication and key management based technique called Hybrid Key Management has been proposed in [57]. Routing protocols play integral part in modern wireless networks so IGRP (Interior Gateway Routing Protocol) based solution is proposed in [60], where routing data is used by router to provide security mechanism against vampire attacks.

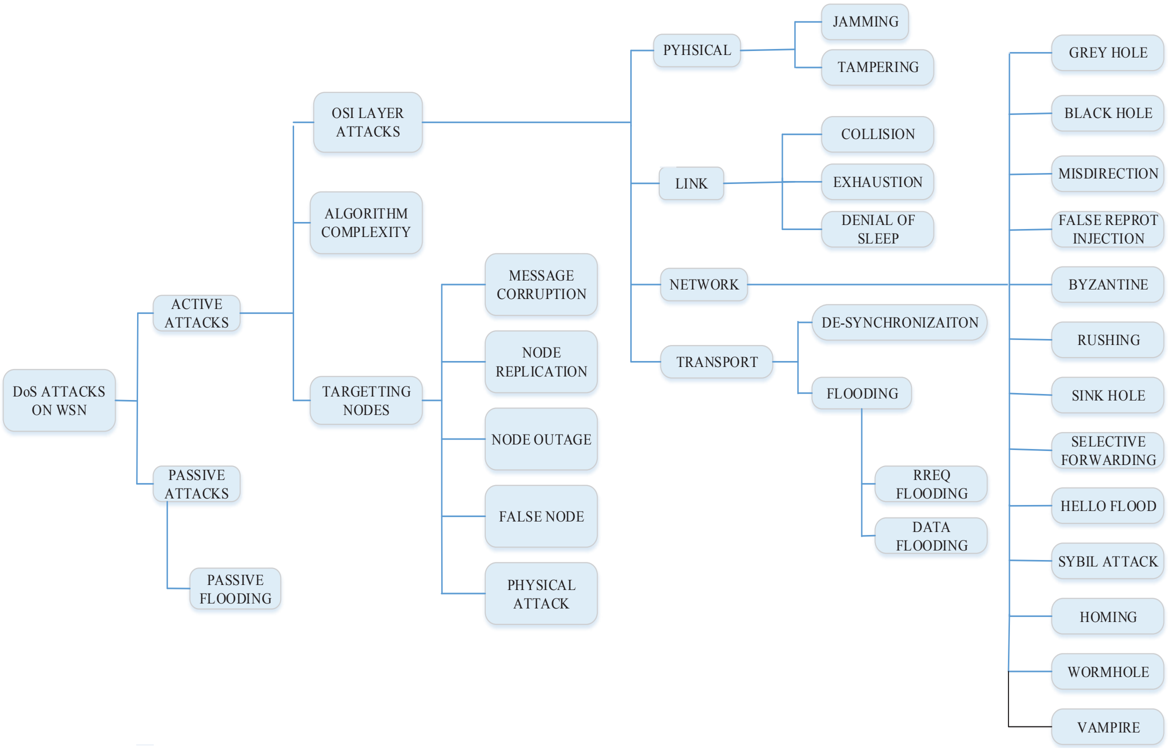
d. **Transport Layer Attacks:** Main threats to the transport layer are Flooding and De-Synchronization attacks[14][12].

Flooding Attacks: Flooding consumes memory of victim node by sending numerous control packets and overflows victim node memory resources. There are two types of flooding attacks. RREQ Flooding Attack: In WSN rate of sending RREQ packets is limited but malicious node does not obliged to send limited packets because it doesn't follow routing protocol rules and can send packet out of limit. The malicious node doesn't wait for RREP packet and resend RREQ. Data Flooding Attack: By setting paths to all nodes malicious node then sends useless data packets to them to consume stack memory. Client Puzzle technique is a solution for flooding attack [13]. Cryptographic puzzles dispersed into the network with the help of beacon frames [61]. IP-layer client puzzle solution also called Chained puzzle protocol actively defend against DoS attacks [62]. Devices suffered from flooding attack recover themselves when attack stops. A reactive technique such as pushback or trace-back is used to lessen the impact of flooding attack. By using game theory client puzzle approach has been applied against flooding and logic attacks [61].

De-Synchronization Attack: In De-synchronization attack, wireless sensor nodes are put into infinite loop by forging messages between nodes [14]. Authorization between network nodes is novel solution to counter these attacks[14]. Content and patch based watermarking techniques helps to prevent against de-synchronization attacks[63]

Table 4: Attacks on Network Layer and Defenses

Attacks	Defenses
Gray Hole	Distributed IDS, ECC based Routing Algorithm, LEACH
False Report Injection	Fuzzy Logic based Authentication, Statistical En-Route Filtering
Wormhole	Flexible Distance Vector Protocol, Challenge bit and Response, AES-AODV
Misdirection	Egress Filtering, Authentication and Authorization of Routing updates, CIC, Cluster based IDS, IPS
Byzantine	ODSBR, Isolation of nodes scheme, ECDSA
Rushing	Dynamic Secure Routing, SMT/SRP Protocol, Anomaly based IDS
Sinkhole	AODV based routing algorithm, Signature based IDS,
Selective Forwarding	Hop by Hop Cooperative Detection, Challenge/Response, SeRINS,
Hello Flood	Tow Way Authentication and Three Way Handshake, Distributed IDS, LEACH,CSMA/CA
Sybil	Authentication, Location Verification
Homing	Encryption, Secure Clustering, Message Hiding
Vampire	PLGPa modification, IGRP, Hybrid Key Management



Future Work

In this segment we present direction for future work to implement more secure and self-organizing techniques to counter DoS attacks in wireless sensor networks. We will discuss some areas in which more secure solution can be created for DoS attacks in WSN.

Learning Based Self-Configuration: Self-configuration technique might use two approaches: Centralized approach and Distributed approach. In centralized fashion each node is configured by some central entity. This approach is stable but limited to small networks, however on large networks distributed approach [64] is more suitable. In this approach every node locally determines its configuration parameters by learning the configuration parameters of its neighboring nodes. This approach might not be good for stability of the network because each node is dependent on reliable transmission of neighboring node configurations. Self-learning techniques like supervised learning are being used in WSN to counter major DoS attacks specially on network layer like Grey-hole, Wormhole and Hello flood attacks [65].

Co-ordination among sensor nodes: Network requires local co-ordination among sensor nodes for more robust and reliable functionalities and it is totally depended on self-organization algorithms. Genetic machine learning algorithm (GMLA) [66] approach might be used to achieve self-organization in WSN which helps to make co-ordination among sensor nodes. It is greatly helpful to counter attacks like Misdirection, Rushing and Node Replication attacks.

Bio-Inspirational Models: Biologically inspired models give healthy relation among biology and computer systems in which computer problems are solved with biological solutions. Reasons to get inspired from these solutions are their adaptive nature to their environment which confirms their survival in hard conditions and resilience against failures. A Human Immune System based bio-inspired model is presented in [67] [68] to mitigate DoS attack in WSN. It gives an idea from the different blood cells functionalities like B-Cells, T-Cells, and Antibodies and maps these functionalities to different nodes such as Sensor nodes, Clustered Head and Gateway Nodes.

Hybrid multi-protocol Solutions: There is need to provide hybrid solution to counter multiple attacks on different layers of WSN. A multi-layer hybrid machine learning based IDS solution is provided for DoS attacks in [69] in which genetic algorithm has been used for anomaly detection. There is also a scope for research in data-mining and hybrid approach using machine learning techniques to provide best solution.

Conclusion

In this survey we classified DoS attack on Wireless Sensor Network and discussed their countermeasure techniques according to the type of attack. Other surveys related to classification of attacks on WSN are available but they do not include such a number of DoS attacks on WSN along with their countermeasures. Some characteristics of WSN which make them vulnerable to DoS attacks are also discussed in this paper. Network layer is the most vulnerable layer for DoS attacks due to defenseless routing algorithms. Research based solutions has also been discussed but there is still a need for more work in this domain which can results in novel solution against variety of DoS attacks.

REFERENCES

1. J. A. Stankovic and A. D. Wood, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of sensor networks: compact wireless and wired sensing systems*, ed: CRC Press, 2004.
2. J. Cai, P. Yi, Y. Tian, Y. Zhou, and N. Liu, "The simulation and comparison of routing attacks on DSR protocol," in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, 2009, pp. 1-4.
3. N. Komninos, D. Vergados, and C. Douligeris, "Layered security design for mobile ad hoc networks," *computers & security,* vol. 25, pp. 121-130, 2006.
4. S. Umrao, A. Kumar, and P. Umrao, "Security attacks and their countermeasures along with node replication attack for time synchronization in wireless sensor network," in *Advanced Nanomaterials and Emerging Engineering Technologies (ICANMEET), 2013 International Conference on*, 2013, pp. 576-581.
5. V. Nigam, S. Jain, and K. Burse, "Profile based scheme against DDoS attack in WSN," in *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*, 2014, pp. 112-116.
6. W. Qiao, J. Li, and J. Ren, "An efficient Error-Detection and Error-Correction (EDEC) scheme for network coding," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1-5.
7. S. Ghormare and V. Sahare, "Implementation of data confidentiality for providing high security in Wireless Sensor Network," in *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*, 2015, pp. 1-5.
8. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications,* vol. 23, pp. 839-850, 2005.
9. V. B. Salve, L. Ragha, and N. Marathe, "AODV based secure routing algorithm against Sinkhole attack in wirelesses Sensor Networks," in *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on*, 2015, pp. 1-7.
10. V. F. Taylor and D. T. Fokum, "Mitigating black hole attacks in wireless sensor networks using node-resident expert systems," in *Wireless Telecommunications Symposium (WTS), 2014*, 2014, pp. 1-7.
11. T.-G. Lupu, I. Rudas, M. Demiralp, and N. Mastorakis, "Main types of attacks in wireless sensor networks," in *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering*, 2009.
12. Y. Jiang, J. Hiiang, and W. Jin, "Intrusion tolerance system against denial of service attacks in wireless sensor network," 2014.
13. X. Ouyang, B. Tian, Q. Li, J.-y. Zhang, Z.-M. Hu, and Y. Xin, "A novel framework of defense system against DoS attacks in wireless sensor networks," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, 2011, pp. 1-5.
14. E. Achuthan and R. Kishore, "A novel anti jamming technique for Wireless Sensor Networks," in *Communications and Signal Processing (ICCSP), 2014 International Conference on*, 2014, pp. 920-924.
15. V. Manju and M. S. Kumar, "Detection of jamming style DoS attack in Wireless Sensor Network," in *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*, 2012, pp. 563-567.
16. A. Azim, S. Mahiba, T. A. K. Sabbir, and S. Ahmad, "Efficient Jammed Area Mapping in Wireless Sensor Networks," *IEEE Embedded Systems Letters,* vol. 6, pp. 93-96, 2014.
17. S. Venkatasubramanian and V. Jothi, "Integrated authentication and security check with CDMA modulation technique in physical layer of Wireless Body Area Network," in *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on*, 2012, pp. 1-6.
18. H.-M. Sun, S.-P. Hsu, and C.-M. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, 2007, pp. 457-462.
19. I. Mandwi, Y. Bute, P. Karmore, and K. Gajbhiye, "Implementation of packet-hiding algorithm for preventing selective jamming attacks," in *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*, 2015, pp. 1-6.
20. N. Joshi, J. Sundararajan, K. Wu, B. Yang, and R. Karri, "Tamper proofing by design using generalized involution-based concurrent error detection for involutional Substitution Permutation and Feistel Networks," *IEEE Transactions on Computers,* vol. 55, pp. 1230-1239, 2006.
21. M. S. Obaidat, I. Woungang, S. K. Dhurandher, and V. Koo, "Preventing packet dropping and message tampering attacks on AODV-based mobile ad hoc networks," in *Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on*, 2012, pp. 1-5.
22. I. Khalil, "MCC: Mitigating colluding collision attacks in wireless sensor networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1-5.

23. P. Reindl, K. Nygard, and X. Du, "Defending malicious collision attacks in wireless sensor networks," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 771-776.
24. S. A. Khan and Z. A. Baig, "On the use of unified and-or fuzzy operator for distributed node exhaustion attack decision-making in wireless sensor networks," in *Fuzzy Systems (FUZZ), 2010 IEEE International Conference on*, 2010, pp. 1-7.
25. 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 transactions on vehicular technology,* vol. 58, pp. 367-380, 2009.
26. D. R. Raymond and S. F. Midkiff, "Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 2007, pp. 1-7.
27. V. Manju, S. S. Lekha, and M. S. Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in *Information & Communication Technologies (ICT), 2013 IEEE Conference on*, 2013, pp. 74-77.
28. S. M. Sakharkar, R. Mangrulkar, and M. Atique, "A survey: A secure routing method for detecting false reports and gray-hole attacks along with Elliptic Curve Cryptography in wireless sensor networks," in *Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on*, 2014, pp. 1-5.
29. I. Almomani and B. Al-Kasasbeh, "Performance analysis of LEACH protocol under Denial of Service attacks," in *Information and Communication Systems (ICICS), 2015 6th International Conference on*, 2015, pp. 292-297.
30. N. Dharini, R. Balakrishnan, and A. P. Renold, "Distributed detection of flooding and gray hole attacks in Wireless Sensor Network," in *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on*, 2015, pp. 178-184.
31. S. P. Dongare and R. S. Mangrulkar, "Implementing energy efficient technique for defense against Gray-Hole and Black-Hole attacks in wireless sensor networks," in *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*, 2015, pp. 167-173.
32. M. S. I. Mamun and A. Kabir, "Hierarchical design based intrusion detection system for wireless ad hoc network," *arXiv preprint arXiv:1208.3772,* 2012.
33. J. H. Kim and T. H. Cho, "Interleaved Hop-by-Hop Authentication using fuzzy logic to defend against of False Report Injection by Replaying an attack," *International Journal of Computer Science and Network Security,* vol. 9, pp. 91-96, 2009.
34. I. Woungang, S. K. Dhurandher, V. Koo, and I. Traore, "Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad Hoc networks," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, 2012, pp. 1037-1041.
35. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," *Department of Computer Science, Johns Hopkins University, Tech. Rep. Version,* vol. 1, p. 16, 2004.
36. J. Soryal, "Byzantine Attack Isolation in IEEE 802 . 11 Wireless Ad- Hoc Networks."
37. P. Zhang, J. Y. Koh, S. Lin, and I. Nevat, "Distributed event detection under byzantine attack in wireless sensor networks," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on*, 2014, pp. 1-6.
38. B. Stelte, "Protection against Byzantine attacks on Wireless Sensor Networks," in *Wireless Information Networks and Systems (WINSYS), 2011 Proceedings of the International Conference on*, 2011, pp. 53-58.
39. J. Xu, K. Wang, C. Wang, F. Hu, Z. Zhang, S. Xu*, et al.*, "Byzantine fault-tolerant routing for large-scale wireless sensor networks based on fast ECDSA," *Tsinghua Science and Technology,* vol. 20, pp. 627-633, 2015.
40. K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," in *Computer Science and Electronic Engineering Conference (CEEC), 2015 7th*, 2015, pp. 231-236.
41. L. Tamilselvan and V. Sankaranarayanan, "Solution to prevent rushing attack in wireless mobile ad hoc networks," in *Ad Hoc and Ubiquitous Computing, 2006. ISAUHC'06. International Symposium on*, 2006, pp. 42-47.
42. A. Rawat, P. Vyavahare, and A. Ramani, "Evaluation of rushing attack on secured message transmission (SMT/SRP) protocol for mobile ad-hoc networks," in *Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on*, 2005, pp. 62-66.
43. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks,* vol. 1, pp. 293-315, 2003.
44. M. Guerroumi, A. Derhab, and K. Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink," in *Information Technology-New Generations (ITNG), 2015 12th International Conference on*, 2015, pp. 307-313.
45. M. A. Rassam, A. Zainal, M. A. Maarof, and M. Al-Shaboti, "A sinkhole attack detection scheme in mintroute wireless sensor networks," in *Telecommunication Technologies (ISTT), 2012*

International Symposium on, 2012, pp. 71-75.

46. S. Lim and L. Huie, "Hop-by-Hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*, 2015, pp. 315-319.
47. C. Kavitha, "A secured alternative path routing protocol against DoS attack," in *Wireless and Optical Communications Networks (WOCN), 2014 Eleventh International Conference on*, 2014, pp. 1-5.
48. P. Sharma, M. Saluja, and K. K. Saluja, "Detection techniques of selective forwarding attacks in wireless sensor networks: a survey," *arXiv preprint arXiv:1205.4905,* 2012.
49. K. Saghar, D. Kendall, and A. Bouridane, "Raeed: A solution for hello flood attack," in *Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on*, 2015, pp. 248-253.
50. M. S. Haghighi, K. Mohamedpour, V. Varadharajan, and B. G. Quinn, "Stochastic modeling of hello flooding in slotted CSMA/CA wireless sensor networks," *IEEE transactions on information forensics and security,* vol. 6, pp. 1185-1199, 2011.
51. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, 2015, pp. 318-325.
52. A. A. Patel and S. J. Soni, "A Novel Proposal for Defending Against Vampire Attack in WSN," in *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*, 2015, pp. 624-627.
53. E. Mariyappan and C. Balakrishnan, "Power draining prevention in Ad-Hoc Sensor networks using sensor network encryption protocol," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, 2014, pp. 1-5.
54. V. Subha and P. Selvi, "Defending against vampire attacks in wireless sensor networks," *International Journal of Computer Science and Mobile Computing,* 2014.
55. E. Y. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," *IEEE transactions on mobile computing,* vol. 12, pp. 318-332, 2013.
56. L. R. Deshmukh, *Of the Vampire Attacks in WSN using Routing Loops*, 2015.
57. R. Abirami and G. Premalatha, "Depletion of vampire attacks in medium access control level using interior gateway routing protocol," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, 2014, pp. 1-5.
58. Q. Dong, L. Gao, and X. Li, "A new client-puzzle based DoS-resistant scheme of IEEE 802.11 i wireless authentication protocol," in *Biomedical Engineering and Informatics (BMEI), 2010 3rd International Conference on*, 2010, pp. 2712-2716.
59. T. J. McNevin, J.-M. Park, and R. Marchany, "Chained puzzles: a novel framework for IP-layer client puzzles," in *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on*, 2005, pp. 298-303.
60. C. Delong, L. Qirui, Y. Guilan, and X. Jianbin, "Content-based audio watermarking method to resist de-synchronization attacks," in *Information and Network Security, ICINS 2014-2014 International Conference on*, 2014, pp. 28-32.
61. S. Rashid, U. Akram, S. Qaisar, S. A. Khan, and E. Felemban, "Wireless sensor network for distributed event detection based on machine learning," in *Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE*, 2014, pp. 540-545.
62. N. J. Patel and R. H. Jhaveri, "Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey," in *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on*, 2015, pp. 468-472.
63. A. R. Pinto, B. Bitencort, M. A. Dantas, C. B. Montez, and F. Vasques, "Genetic machine learning approach for data fusion applications in dense Wireless Sensor Networks," in *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*, 2008, pp. 1177-1180.
64. H. Rathore and S. Jha, "Bio-inspired machine learning based wireless sensor network security," in *Nature and Biologically Inspired Computing (NaBIC), 2013 World Congress on*, 2013, pp. 140-146.
65. H. Rathore, V. Badarla, S. Jha, and A. Gupta, "Novel approach for security in wireless sensor network using bio-inspirations," in *Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on*, 2014, pp. 1-8.
66. A. S. A. Aziz, A. E. Hassanien, S. E.-O. Hanaf, and M. F. Tolba, "Multi-layer hybrid machine learning techniques for anomalies detection and classification approach," in *Hybrid Intelligent Systems (HIS), 2013 13th International Conference on*, 2013, pp. 215-220.