International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Energy Depletion Attacks in Wireless Sensor Networks

Dr. N. Geethanjali[1], E. Gayathri[2]

[1]Associate Professor, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India

[2]Research Scholar, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India

Abstract: ***Wireless Sensor Network (WSN), a collection of mobile nodes, is vulnerable to various attacks due to their mobility and resource constrained nature. As this network and its applications became ubiquitous for machine critical applications, it is indispensable to safeguard its communications in energy efficient fashion. Availability of such network is crucial for productivity. Wireless Ad Hoc Sensor Networks are vulnerable Denial of Service (DoS) is the that cause short term unavailability of network. However, the attacks that affect long term availability of the network are resource depletion attacks that cause more damage to the applications for which availability of network is important. This paper presents QoS issues and energy depletion issues and the countermeasures employed. As security QoS, and availability of network are to be given paramount importance, this paper provides insights into the present state of the art pertaining to resource depletion attacks and prevention methods employed.***

Keywords: depletion, energy, wireless sensor networks

1. Introduction

Wireless Sensor Network (WSN) is a network of wireless nodes or sensors that sense data in pre-defined fashion. WSNs are widely used for machine critical applications in civilian, military and research fields. They can be used for space research, studying wildlife habitat in forests, target tracking in military operations, observation of households, study of environment and so on [1]. In such applications the life of network and Quality of Service (QoS) plays crucial role in accomplishing the intended goals of the network. As the nodes have limited resources and often have mobility nature they are vulnerable to various kinds of attacks. These attacks can be classified into two categories active and passive attacks. An active attack refers to the attack that causes unauthorized changes to the system or data in the network. For instance Denial of Service (DoS) attacks is an example for such attack. Passive attack is the attack where an adversary indirectly listens to communication traffic in networks. In other words interception of messages without modification comes under passive attack. Reader can find a good review of active and passive attacks in WSN in [5]. QoS is in jeopardy when WSN is subjected to attacks. There are QoS based routing protocols that enhance reliability of communications in WSN. They include EQSR, MCBR, MCMP, MMSPEED, and SAR as explored in [13]. As mentioned earlier both QoS and energy efficiency are to be given paramount importance in WSN. In this perspective the security goals of WSN are Confidentiality, Integrity, Authentication and Availability (CIAA). Confidentiality refers to the ability to conceal messages from eavesdropping. Authentication refers to the verification of the origin of message to be valid. Integrity refers to the correctness of data which is not modified on transit. Availability refers to the network and its resource availability to nodes to perform their intended functionality. Reader can find more information on security goals in [1].

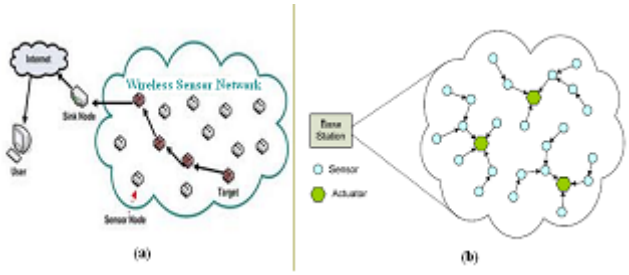

Figure 1: Shows WSN (a) and WSAN (b)

Sensor nodes base station are involved in WSN (a) while an additional entity known as actuator is involved in WSAN (b). Sensor is meant for gathering information from physical world while the actuator makes decision to react based on sensed information. In this paper our focus is on energy depletion attacks in WSN. This is the area where more research is required as energy depletion leads to reduction of network life time.

Our contribution in this paper is the study of review of energy depletion attacks and QoS issues in Wireless Sensor Networks. The study reveals important insights and research gaps that can help in taking the research on WSN forward. The remainder of this paper is structured as follows. Section 2 reviews energy depletion issues in WSNs. Section 3 focuses on attacks in WSN and also Quality of Service (QoS) issues in WSN. Section 4 presents research gaps found from the insights of this paper while section 5 concludes the paper.

2. Energy Depletion Issues in WSNS

Since energy efficiency is crucial in resource constrained network like WSN, this section reviews the issues and solutions with respect to energy depletion attacks in WSN. Ren et al. (2009) [6] proposed multi-user broadcast authentication using security aspects like Merkle hash

tree, bloom filter and partial message recovery signature. This solution prevents energy depletion attacks. It overcomes the drawbacks of prior symmetric based solutions such as "μTESLA" [36] besides reducing computational and communication costs. Khouzani and Sarkar (2010) [9] explored malware outbreaks in WSN and possible solutions to avoid energy depletion due to such attacks. They used Pontryagin's maximum principle for finding optimal solution towards battery depletion attacks in WSN. Their solution makes use of the notion of state transitions (Figure 2) so as to use counter-measures for energy – depletion attacks.

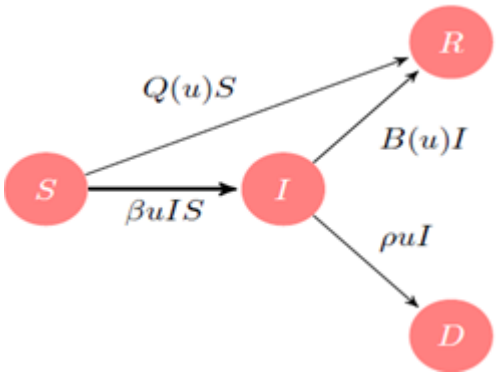

Figure 2: State transitions [9]

The states such as S, I, R, D represents susceptible, infective, recovered and dead states. While data or control messages are being transmitted, malware spread may occur. This leads to various problems including energy-depletion attack. Kaleeswar and Baskaran (2012) [14] proposed a new routing protocol to overcome the energy issues. The algorithm is named Aware Energy Balanced Dynamic Routing Protocol (DA-EBDRP). This is a routing technique which is energy efficient besides delay sensitive in nature. Energy balanced shortest route finding is the salient feature of this technique.

2.1 Vampire Attacks in Wireless Sensor Networks

Vampire is nothing but a compromised node in WSN. Through this node adversary can send protocol compliant messages to other nodes continuously and let them answer the messages so as to ensure that each node in the network looses energy faster (energy depletion) causing the failure of the whole network soon. Recently more focus was in given in the research on vampire attacks and solutions. Vasserman and Hopper (2013) [16] explored resource depletion attacks in ad hoc sensor networks. They studied all routing protocols and found that vampire attacks can target any routing protocol. Detecting vampire attack is difficult as only one malicious insider in the network causes this attack by sending protocol-compliant messages. They proposed a new protocol to detect and vampire attack thus preventing energy depletion in Ad Hoc WSN. They could identify two kinds of attacks in tasteful protocols such as OLSR [37] and DSDV [38] which are examples for link-state and distance vector protocols respectively. The attacks are known as directional antenna attack and malicious discovery attack. Spurious route discovery is the main theme of the latter while the former wastes energy by restarting packets unnecessarily. Their study on stateless protocols identified two attacks such as Carousel attack and Stretch attack found in routing protocol DSR [39]. In case of Carousel attack a hacker sends a packet to a route made up of multiple unnecessary loops. In case of Stretch attack the compromised node creates artificial source routes which are very log. In these two cases unnecessary traffic from various nodes in the network causes energy depletion. The honest scenario, Carousel attack scenario and Stretch attack scenario are presented in Figure 3.

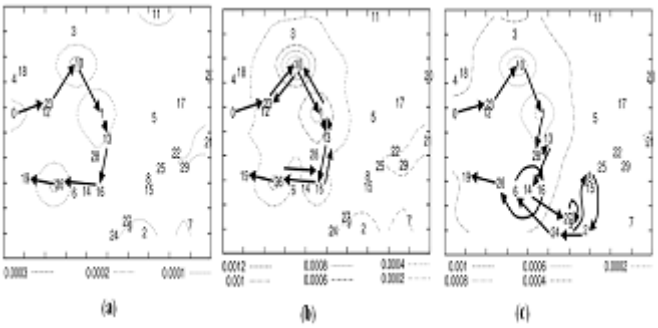

Figure 3: Honest scenario (a), Carousel attack scenario (b) and Stretch attack scenario (c) [16]

The honest route between sender (0) to receiver (19) packets is sent as shown in Figure 3 (a). Figure 3 (b) shows unnecessary looping in routing and the node 0 is considered malicious node. In Figure 3 (c) it can be seen that extra routing is created which is quite unnecessary causing stretch of the original routes. The scenarios described in (b) and (c) are causing unnecessary traffic from WSN nodes in protocol-compliant fashion causing energy depletion. The energy usage dynamics under various attacks and honest scenarios is presented in Figure 4.

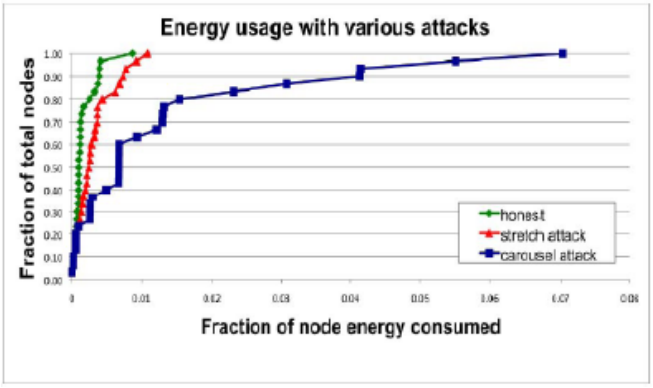

Figure 4: Energy usage dynamics under attacks and honest behavior [16]

The energy consumption with carousal attack is very high when compared with stretch attack. The reason behind this is that the carousal attack causes more loops while routing packets while the stretch attack uses simple extended routes to the existing ones. As shown in the graph the energy consumption in honest scenario is far lesser than the two attack scenarios. Research on vampire attacks is also found in [15], [17], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], and [34].

Hosamsoleman et al. (2013) [18] focused on collision attacks in WSN. This attack is made at link layer of the network. Rate limitation and error correcting code are the possible solutions to this problem. Umakanth and Damodhar (2013) [19] presented Energy Weighted Monitoring Algorithm (EWMA) method in preventing vampire attacks targeted at routing protocols. Mitchel and Chen (2014) [20] provided insights into various attacks in wireless network applications.

2.2 Energy Depletion Issues in WSN

Author (s)	Year	Solution	Study	Method/Technique	Remarks
Ren *et al.* [6]	2009	Multi-user broadcast authentication	Simulation	Merkle hash tree, Bloom filter, partial message recovery signature scheme.	Prevents energy depletion attacks
Khouzani and Sarkar [9]	2010	Solution for battery depletion attack in WSN	Simulation	**Pontryagin's maximum principle**	Notion of states such as infective, susceptible, recovered and dead are used
Kaleeswar and Baskaran [14]	2012	Energy balancing in WSN	Simulation	Energy Balanced Dynamic Routing Protocol	Improved throughput, delay performance and network life time
Vasserman and Hopper [16]	2013	Clean-slate secure sensor network routing protocol	Simulation	Modified PLGP[55]	Protocol independent attacker model
Hosamsoleman *et al.* [18]	2013	Detection of energy draining attack	Simulation	EWMA	-

3. Quality of Service Issues and Other Attacks in WSNs

Quality of Service (QoS) is the active research area in WSN. Felemban et al. [1] proposed a novel packet delivery mechanism for improving QoS. Multi-path and Multi-Speed Routing Protocol (MMSPEED) was proposed by them for QoS provisioning in reliability and timeliness domains. Lee [2] proposed an adaptive QoS for wireless ad hoc networks. A signaling protocol named INSIGNIA for congestion mitigation and cost-efficient routing mechanism was proposed for enhancing QoS in sensor networks. Kaplantzis et al. (2007) [3] studied selective forwarding attacks in WSN. They proposed a centralized Intrusion Detection System (IDS) using Support Vector Machines (SVM). These IDS could also detect black hole attacks besides causing depletion of energy. Xia (2008) [4] studied QoS challenges and opportunities in WSAN. Their research was on QoS requirements such as throughput, delay, and jitter and packet loss rate. QoS issues and solutions are also explored in [7], [8], [10], and [11]. In [11] QoS is studied in presence of heterogeneous WSN. QoS support at MAC layer of protocols is explored in [12] where service differentiation was found to be the approach followed by protocols. QoS based routing protocols are reviewed in [13] performance metrics such as reliability, end-to-end delay, energy efficiency, control packet overhead and network lifetime are studied with protocols such as EQSR, MCBR, MCMP, MMSPEED, and SAR. EQSR was reported to have highest reliability against density.

3.1 Summary of QoS Research in WSN

Author (s)	Year	Solution	Study	Method/Technique	Remarks
Kaplantzis *et al.* [3]	2007	IDS to prevent selective forwarding and black hole attack.	Simulation	SVM classifier	DoS attacks were studied
Aykut *et al.* [12]	2011	Qos-Aware MAC protocols	Simulation	Service differentiation approach	Deterministic QoS guarantees are given less importance

4. Research Gaps Found

The solution in [3] can be improved by investigating the tradeoff between detection accuracy and energy depletion in WSN. The solution in [9] for preventing energy depletion attacks can be evaluated through empirical study using a test bed. QoS provisioning in WSNs can be improved at MAC layer of protocols [12]. In [16] solution was provided for vampire attacks. However, with respect to topology discovery phase, it is not fully satisfactory. It is possible to derive damage bounds for topology discovery besides devising defenses for more robust solution.

5. Conclusions and Future Work

In this paper we studied QoS issues and resource depletion attacks in Wireless Sensor Networks. As the nodes in such network are susceptible to various kinds of attacks, it is essential to have counter measures to ensure security goals of network such as confidentiality, integrity, authentication and availability. Availability of Wireless Ad Hoc Sensor Network is crucial for achieving its intended goals in machine critical applications in civilian and military operations. The applications of sensor networks became important for productivity of organizations. Security is the major concern in such networks where nodes are vulnerable to various kinds of attacks. In this paper we focused on QoS issues and resource depletion attacks in WSNs. This paper also provides insights into the state-of-the-art of Wireless Ad Hoc Sensor Networks with respect to threats and counter measures. The research gaps are found which can help in taking the research forward on WSN with respect to energy depletion attacks and solutions. In future we work on proposing a novel protocol WSN which further reduces the chances of resource depletion attacks.

References

[1] Emad Felemban, Chang-Gun Lee, Eylem Ekici, Ryan Boder, and Serdar Vural. (2005). Probabilistic QoS Guarantee in Reliability and Timeliness Domains in Wireless Sensor Networks. ieee. . (n.d), p-1-12.
[2] Seoung-Bum Lee. (2006). Adaptive Quality of Service for Wireless Ad hoc Networks. (n.d), p-1-236.
[3] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani and Y. Ahmet ekercioglu. (2007). Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines. ieee (n.d), p-335-340.
[4] Feng Xia. (2008). QoS Challenges and Opportunities in Wireless Sensor/Actuator Networks. (n.d), p-1-12.
[5] Dr. G. Padmavathi and Mrs. D. Shanmugapriya. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. ijcsis. 4 (n.d), p-1-9.
[6] Kui Ren and Wenjing Lou,. (2009). Multi-User Broadcast Authentication in Wireless Sensor Networks. ieee. 58 (n.d), p-4554-4564.
[7] RAJSHREE and S. DUBEY1. (2010). Challenges for Quality of Service (QoS) in Wireless Sensor Networks. ijest. 2 (n.d), 7395-7400
[8] S.Muthukarpagam,V.Niveditta and S.Neduncheliyan . (2010). Design issues, Topology issues, Quality of Service Support for Wireless Sensor Networks: Survey and Research Challenges. ijcat. 1 (n.d), p-1-4.
[9] M.H.R. Khouzaniand Saswati Sarkar. (2010). Maximum Damage Battery Depletion Attack in Mobile Sensor Networks. (n.d), p-1-12.
[10] Bhaskar Bhuyan, Hiren Kumar Deva Sarma, Nityananda Sarma, Avijit Kar and Rajib Mall. (2010). Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges. scientific research. 2 (n.d), p-861-868.
[11] Majid Nabi, Milos Blagojevi, Marc Geilen and Twan Basten. (2011). Dynamic Data Prioritization for Quality-of-Service Differentiation in Heterogeneous Wireless Sensor Networks. ieee. (n.d), p-217-225.
[12] M. Aykut Yigitel , Ozlem Durmaz Incel and Cem Ersoy. (2011). QoS-aware MAC protocols for wireless sensor networks: A survey. elsevier. 55 (n.d), p-1983-2004.
[13] R.Sumathi and M.G.Srinivas. (2012). A Survey of QoS Based Routing Protocols for Wireless Sensor Networks. J Inf Process Syst,. 8 (n.d), p-589-603.
[14] N.Kaleeswari and Dr.K.Baskaran. (2012). Implementation of Energy Balancing in Wireless Sensor Networks. ijcsi. 9 (n.d), p-553-560.
[15] Mrs.Priti Lale(Lahane) and Dr. G.R. Bamnote. (2013). Detecting and preventing vampire attack in wireless sensor network. ijser. 4 (n.d), p-408-411.
[16] Eugene Y. Vasserman and Nicholas Hopper. (2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. ieee. 12 (n.d), p-1-15.
[17] Mrs.Priti Lale(Lahane) and Dr. G.R. Bamnote. (2013). Detecting and preventing vampire attack in wireless sensor network. ijser. 4 (n.d), p-408-411.
[18] Hosamsoleman, Ali Payandeh, Nasser Mozayyani and SaeedSedighianKashi. (2013). Detection Collision Attacks In Wireless Sensor Network Usingrule-Based Packet Flow Rate. ijera. 3 (n.d), p-261-268.
[19] B. Umakanth, J. Damodhar. (2013). Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks. IJETT. 4 (n.d), p-1-5.
[20] Robert Mitche and Ing-Ray Chen . (2014). A survey of intrusion detection in wireless network applications. elsevier. 42 (n.d), p-1-23.
[21] Farzana T and Aswathy Babu. (2014). Energy Depletion Attacks on Wireless Sensor Networks: A Survey. ijcat. 1 (n.d), p-45-48.
[22] Tawseef Ahmad Naqishbandi and Imthyaz Sheriff. (2014). A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT.ijarcsse. 4 (n.d), p-766-773.
[23] Ambili M , BijuBalakrishnan. (2014). A Security Approach For Detection And Elimination Of Resource Depletion Attack In Wireless Sensor Network. ijircce. 2 (.), p-1-6.
[24] P.Rajipriyadharshini,V.Venkatakrishnan,S.Suganya, and A.Masanam. (2014). Vampire Attacks Deploying

Resources in Wireless Sensor Networks. ijcsit. 5 (n.d), p-2951-2953.
[25] K.Vanitha and V.Dhivya. (2014). A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks. ijirset. 3 (n.d), p-2441-2446.
[26] Vidya and M Reshmi.S. (2014). Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks. ijirae. 1 (n.d), p-1-5.
[27] Vidya M and Reshmi. (2014). Denial of Service Attacks in Wireless Sensor Networks. ijacte. 3 (n.d), p-16-21
[28] P.Suthahar and R.Bharathi. (2014). Defending against Energy Draining attack in Wireless Ad-Hoc Sensor Networks. ijarcst. 2 (n.d), p-420-425.
[29] SHARNEE KAUL, HELEN SAMUEL, JOSE ANAND3. (2014). DEFENDING AGAINST VAMPIRE ATTACKS IN WIRELESS SENSOR NETWORKS. ijcea. 5 (n.d), p-566-571
[30] Vidya and M Reshmi.S. (2014). Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks. ijirae. 1 (n.d), p-1-5.
[31] S. ARVIND KUMAR and Mrs. DEEPA DIVAKARAN. (2014). DETECTING AND AVOIDING NETWORK ATTACKS USING ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS. COMPUSOFT, An international journal of advanced computer technology,. 3 (n.d), p-1-3.
[32] K.Sivakumar and P.Murugapriya. (2014). Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks.ijircce. 2 (n.d), p-596-600.
[33] Farzana T and Aswathy Babu. (2014). Energy Depletion Attacks on Wireless Sensor Networks: A Survey. ijcat. 1 (n.d), p-45-48.
[34] Soram Rakesh Singh and Narendra Babu C R. (2014). improving the performance of energy attack detection in wireless sensor networks for secure forward mechanism. ijsrp. 4 (n.d), p-1-5.
[35] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocols for sensor networks," in Proc. MobiCom, Rome, Italy, Jul. 2001, pp. 189–199.
[36] T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.
[37] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. Conf. Comm. Architectures, Protocols and Applications, 1994.
[38] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.
[39] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006dix

Acronym Description

WSN: Wireless Sensor Network
QOS: Quality of Service
CIAA: Confidentiality, Integrity, Authentication and Availability
MMSPEED: Multi-path and Multi-Speed Routing Protocol
WSAN: Wireless Sensor and Actuator Network
DA-EBDRP: Energy Balanced Dynamic Routing Protocol
EWMA: Energy Weighted Monitoring Algorithm