





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 <i>et al.</i> [6]	2009	Multi-user broadcast authentication	Simulation	Merkle hash tree, Bloom filter, partial message recovery signature schema.	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
Vaserman and Hopper [16]	2013	Clean-slate secure sensor network routing protocol	Simulation	Modified PLGP[55]	Protocol independent attacker model
Hosamsoleman <i>et al.</i> [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 WSN. 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 <i>et al.</i> [3]	2007	IDS to prevent selective forwarding and black hole attack.	Simulation	SVM classifier	DoS attacks were studied
Aykut <i>et al.</i> [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. Khouzani and 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 Saeed Sedighian Kashi. (2013). Detection Collision Attacks In Wireless Sensor Network Using rule-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, Biju Balakrishnan. (2014). A Security Approach For Detection And Elimination Of Resource Depletion Attack In Wireless Sensor Network. *IJRCSSE*. 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. *ijrset*. 3 (n.d), p-2441-2446.
- [26] Vidya and M Reshmi.S. (2014). Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks. *ijrae*. 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. *ijarct*. 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. *ijrae*. 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. *ijrcc*. 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
- 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

## Acronym Description

WSN: Wireless Sensor Network

QOS: Quality of Service

CIAA: Confidentiality, Integrity, Authentication and Availability