Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.231 – 243

RESEARCH ARTICLE

A Study on Various Attacks in Wireless Ad hoc Sensor Network

Savitha.M[1], Dr. R.Manavalan[2]

[1]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India
[2]Department of Computer Applications, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India
[1] mailme.savi5star@rediffmail.com ; [2] manavalan_r@rediffmail.com

---

ABSTRACT--- Wireless Ad-hoc sensor Networks (WASNs) are networks of light-weight sensors that are battery powered, majorly used for monitoring purposes. It consists of number of sensors that are spread across a geographical area. Many issues are acquired in WASN, such as Energy Efficiency, Limited storage and computation, Low bandwidth, high error rates, scalability to a large number of sensor nodes, Survivability in harsh environments, experimental time and space intensive. Many research papers have been presented so for to overcome these issues. This paper summarizes the various types of attacks and prevention and detection methods in wireless ad hoc sensor networks.

I. INTRODUCTION

Wireless Ad-hoc Sensor Networks are networks that consist of sensors which are distributed in an Ad hoc manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. The number of protocols and algorithms with self-organizing capabilities plays a vital role in Wireless sensor networks.

On demand computing power, continuous connectivity and instantly deployable communication for first responders and military are the new exciting applications presented in Wireless Ad Hoc Sensor Networks [1]. All sensor nodes have typically several parts such as a radio transceiver with an internal antenna or connection to an

external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source for effective communication.

In WASN, Topology plays a vital role for minimizing various constraints, such as limited energy, latency, computational resource crisis and quality of communication. The major issues of wireless ad hoc sensor networks are less security routing, low access control, coverage problem and less energy efficiency and security. To expand the lifetime of the networks and also to preserve a balanced energy expenditure of nodes in Ad-hoc wireless sensor network are still the challenging issues.

WASN with resource constrained nodes makes them very much vulnerable to variety of attacks. The parameter such as throughput, packet end-to-end delay and network load are used to evaluate the performance of the protocols and methods. The rest of the paper is organized as follows: Section II provides brief survey about the attacks in Wireless Ad Hoc Sensor Network. Issues in the attacks are discussed in section III and the conclusion is presented in section IV.

II. ATTACKS IN WIRELESS AD HOC SENSOR NETWORK: A REVIEW

In 2000, Wendi Rabiner Heinzelman et al., [1] presented Low-Energy Adaptive Clustering Hierarchy (LEACH) clustering-based protocol to minimize energy dissipation in sensor networks. In the conventional protocols, direct transmission, minimum transmission energy, multi hop routing and static clustering may not be optimal for sensor networks. To solve these issues, LEACH uses localized coordination to enable scalability and robustness for dynamic networks and also incorporated data fusion into the routing protocol to reduce the amount of information while transmitting to the base station. The results showed that the LEACH reduced the communication energy compared with direct transmission and minimum energy routing transmission.

In 2001, Seapahn Meguerdichian et al., introduced the exposure-based coverage model. Identification of coverage is one of the fundamental problem in networks. The developed algorithm completes the exposure of sensor networks and the same is specifically used to find minimal exposure paths. The algorithm has three main parts: Transform the continuous problem domain to a discrete one, apply graph-theoretic abstraction and Compute the minimal exposure path. Generally Djikstra's Single-Source-Shortest-Path algorithm is used to find the minimal exposure path and the same is replaced by the Floyd-Warshal All-Pair-Shortest-Path algorithm. The results showed that, the algorithm has produced the high quality of results based on the intensity models such as cross, square, triangle and hexagon [2].

In 2002, Arati Manjeshwar et al., Proposed a hybrid routing protocol; **A**daptive **P**eriodic **T**hreshold-sensitive **E**nergy **E**fficient Sensor **N**etwork Protocol (APTEEN) [3] for comprehensive information retrieval. Query handling is one of the main problems in LEACH protocol. Once the CHs are determined for each cluster period, the cluster head broadcasts the parameters such as, attributes, thresholds and schedule and count time. In the protocol, two approaches were used for query handling, flat topology and a cluster based approach. Based on performance

metrics, the results showed that the protocol provides lower dissipation value of energy and a higher number of alive nodes at any given time.

In 2002, Wei Ye et al., presented the sensor-MAC (S-MAC) [4] protocol to reduce the energy consumption. S-MAC uses three techniques periodic listen and sleep, collision and overhearing avoidance and message passing to reduce energy consumption and support self-configuration. In the message passing module, two functions are incorporated periodically such as periodic listen and sleep. Compared with TDMA, all the nodes in S-MAC are free to choose their own listen or sleep schedule. The results demonstrated that, the S-MAC protocol achieved better energy conserving properties compared to IEEE 802.11.

In 2002, Rahul C. Shah et al., [5] proposed a scheme called energy aware routing that uses sub-optimal paths occasionally to provide substantial gains. In sensor networks, resources are limited in sensor network are which is the main issue. To address the issue, the routing protocol is proposed that is suitable for low energy and low bit rate networks. Probabilistic forwarding is used to send the traffic on different routes and provides an easy way to use multiple paths without adding much complexity at a node. Results showed that the protocol increased the lifetime of routing, reduced the overhead and the energy differences between the nodes are also reduced.

In 2003, Vaidyanathan Ramadurai et al., [6] proposed localization algorithm for Ad-hoc sensor networks. Localization is the problem of estimating the spatial coordinates of wireless nodes. To overcome the issue, Robust and RF signal strength based distributed algorithms are used for localizing wireless sensor nodes. The position estimation method is the good way to broadcast the message to all of its neighbours. Simulation results showed that, the estimated position is found accurately with a range of inaccuracy.

In 2003, Roozbeh Jafari et al., [7] presented the energy skew routing algorithm in lossy sensor networks. Extension of the sensor nodes life time is the main issue in sensor networks. In a specific traffic pattern, specific node serves as the gateway or base station. The intermediate nodes are connected to a dummy node to reduce the lossy rate. The lossy flow determines the energy consumption at the sensor nodes. The results showed that, the technique is more efficient to maximize the lifetime and decrease the latency.

In 2003, Yih-Chun Hu et al., [8] designed the Secure Efficient Ad-hoc Distance vector routing protocol (SEAD). This protocol spreads new routing information in networks. The hash tree property is used to authenticate the node ID in the protocol and Merkle tree is used to generate the collection of values. Four metrics were used to evaluate the performance of SEAD protocol such as packet delivery ratio, byte overhead, packet overhead and median overhead. The simulation results showed that the SEAD protocol reduced the overhead of the network.

In 2003, Seema Bandyopadhyay and Edward J. Coyle [9] proposed a randomized clustering algorithm to organize the sensors in a wireless sensor network into clusters. The algorithm works in a bottom-up fashion. It is used to generate a hierarchy of cluster heads and also observed that the energy savings are increased while the number of levels in the hierarchy is increased. In every communication, 1 unit of energy is spent for 1 unit of data. Simulation results showed how the energy consumption decreases while number of the hierarchy level is increased.

In 2003, Chris Karlof et al., [10] proposed a secure routing idea in sensor networks. For analysing the routing security, two classes of attacks against sensor networks sinkholes and Hello floods are introduced. Crippling attacks and counter measures are used for design. The counter measures are described between the parse of outsider and insider attacks. The simulation results showed that the proposed schemes give the better routing and also protect the data from outside attackers.

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes. In 2003, Haowen Chan et al., [11] presented three mechanisms for key establishment; q composite keys scheme, the multipath-reinforcement scheme and the random-pair wise keys scheme. The basic random key predistribution scheme consists of two phases: initialization phase and setup phase. The effectiveness of (2-hop) multipath key reinforcement is evaluated by deploying the random uniform deployment of sensor nodes on a square planar field. From the results, it was observed that the q-composite scheme significantly improved the security under small scale attack whereas the (2-hop) multipath reinforcement scheme improved the security at the cost of network communication overhead.

In 2004, Ossama Younis et al., [12] proposed a distributed clustering approach for long-lived Ad hoc sensor networks. HEED protocol, which terminates in a constant number of iterations, is independent of network diameter. In HEED, intracluster and intercluster routing are used for single hop communication. To increase the energy efficiency and prolong network lifetime, intracluster "communication cost" is considered as a secondary clustering parameter. Simulation results clearly demonstrated that, the HEED prolongs network lifetime since produced clusters exhibit several appealing characteristics. HEED creates a connected multi hop intercluster network effectively when a specified density model and a specified relation between cluster range is in transmission range.

In 2004, Imad Aad et al., [13] presented the design and study of DoS attacks. First attack is JellyFish (JF) attack, the key principle that JF use to facilitate the attack is targeting end-to-end congestion control. The second is the Black Hole attack, Black Hole nodes participate in all routing control plane operations. It employed a broad set of security and DoS resilience mechanisms that (i) ensure node authentication, (ii) ensure message authentication,(iii) ensure one identity per node and (iv) prevent control plane misbehaviour . From this study, these attacks are described in a variety of settings and have provided a quantification of the damage they can inflict.

In 2004, Timothy J. McNevin et al., [14] presented the design of a client puzzle protocol to provide the security in networks. pTCP is a modification of TCP and the goal of the algorithm is to create as much diffusion as possible by incorporating many rounds or iterations of client puzzle operations. pTCP implemented a three-way handshake method to establish a connection between nodes. The results showed that pTCP performed more effective in defending against synflood attacks and syncookies.

In 2004, Xiang Ji et al., [15] presented the multi scaling method for sensor positioning. In order to estimate the accurate position and reduce the error commutation, multidimensional scaling and coordinate alignment techniques are applied to recover positions of adjacent sensors. Further, demand position estimation method based on multidimensional scaling is also introduced for one or several adjacent sensors positioning. Experimental results

indicated that the distributed method for sensor position estimation is very effective and efficient than other positioning methods.

In 2005, Stefan Schmidt and Holger Krahn [16] proposed security architecture for wireless sensor networks to prevent many attacks. The prototypes of the architecture are implemented in the sensor nodes for security. To communicate securely, every node generated a random key within its neighbourhood. The key is used solely by the node to encrypt and authenticate its messages. Generally, Blundo-et-al scheme is used to achieve the pair wise key agreement based on a predistribution scheme. The results show that the implemented prototype provided lightweight solution and is applicable for self-organizing mobile wireless sensor networks.

In 2004, Haibin Sun et al., [17] presented a distributed and efficient approach to dynamically detect and defend against low-rate TCP attacks in network. The developed detection mechanism identifies the existence of low-rate attack in some extent. When the low-rate attack is present, a push back mechanism is used to identify the attack as close to the source of attack as possible. The round-robin approach is used to protect the TCP flows and isolate them from the traffic attack. The simulations exposed the merits and effectiveness of the proposed defence mechanism and the robustness and accuracy of the proposed detection algorithm.

In 2005, Yih-Chun hu and Adrian Perrig [18] presented the secure on-demand routing protocol for ad-hoc networks. The protocol provides security against one compromised node and arbitrary active attackers and relies only on efficient symmetric cryptographic operations. The protocol has designed based on the basic operation of the DSR protocol. The designed security mechanisms are highly efficient and robust. Experimental results showed that, the Ariadne actually performed in terms of metrics than the unoptimized DSR.

In 2005, Li Qing et al., [19] proposed Distributed Energy-Efficient Clustering (DEEC) scheme for heterogeneous wireless sensor networks. To reduce the energy consumption, it is necessary to increase the scalability and lifetime of the network. DEEC estimated the ideal value of network life-time, which is used to compute the reference energy for each node. The results showed that when compared with LEACH-E the DEEC has performed well in multi-level heterogeneous wireless sensor networks.

In 2005, Ping Ding and Aslihan Celik [20] proposed a Distributed, Weight-based Energy-Efficient Hierarchical Clustering algorithm (DWEHC). DWEHC runs in $O(1)$ time which is the major advantage for a power-constrained sensor network. The ideal value of network life-time is estimated to compute the reference energy of each node. In the proposed scheme, six parameters are used to calculate the minimum energy path. These parameters are Relay, Neighbours Relay, Region, Enclosure Region, Cluster range (cluster radius) and Weight. Simulations demonstrated that the DWEHC generated well balanced clusters and also both clusters energy consumption is greatly improved by HEED-AMRP algorithm.

In 2006, Richard Han and Shiva Kant Mishra [21] proposed a solution, using One-way Hash Chains (OHC) to protect end-to-end multi hop communications in WSNs against Path-based DoS (PDoS) attacks. OHC included a skipjack-based one-way function to generate the OHC number. The robustness and reliability of multipath routing has improved for data communications. In routing, every node forwards a packet containing the same OHC number equal to the number of paths. The simulation result showed that the scheme is feasible in current sensor network platforms and solve the overhead within range.

In2006, Sencun Zhu et al., [22] proposed a Lightweight Hop by hop Authentication Protocol for Ad hoc networks. It is a network access control protocol for preventing resource consumption attacks. The LHAP is based on two techniques: (i) hop by hop authentication (ii) one-way key chain. The Time Efficient Streamed Loss-tolerant Authentication (TESLA) is used to reduce the number of public key generation operations for boots trapping trust between nodes. Three protocols were analysed to detect the attacks and the simulations showed that the LHAP is more efficient and provide high security from the attacks.

In 2007, Mujdat Soyturk et al, [23] presented the Stateless Weight Routing with Multiple Sinks (MS-SWR) protocol to reduce the energy consumption and to extend the lifetime of the network. The MS-SWR protocol is scalable protocol for large size networks. It is also reactive stateless geographical routing protocol working independent from the MAC-layer. The energy consumption between stationary sink nodes and mobile nodes in routing is analysed and compared. From the results, it is observed that mobile sinks in routing reduces the energy consumption in a considerable amount.

In 2007, Vahid Shah Mansouri, and Vincent [24] presented the Distributed Maximum Lifetime Routing for Wireless Sensor Networks based on Regularization. Regularization function has satisfied the three properties such as, it is a strictly convex function, it is a separable function and it has a physical interpretation. Additionally, regularization functions and delay function are used for minimizing the total power consumption to satisfy the properties. Simulations are conducted for the comparison of different problems for routing paths, such as fully distributed method, Regularized problem with power term and Regularized problem with delay term. Results showed that the proposed algorithm with regularized power term provided a lower normalized power consumption than the other two schemes.

In 2009, Buyanjargal Otgonchimeg et al., [25] proposed an "Efficient Algorithm for Event-Driven Wireless Sensor Networks (EAED) for prolonging the lifetime of a sensor network by balancing energy usage of the nodes. EECED comprise, of three main phase such as the initial phase, the clustering phase and the data transmission phase. The network lifetime is defined as the round interval from the start of operation until the death of the last alive node. The results exposed that the proposed method has maintained a balanced energy consumption distribution among all the nodes in a sensor network and thus prolong the network lifetime.

In 2009, Allan I. McInnes et al., [26] presented the Flooding Time Synchronization Protocol (FTSP) to restrict the size of the model state-space. Five properties are checked by FTSP model to apply the flooding. Then a number of abstraction techniques are used to keep the small state-space model. Results showed that the FTSP model performed well in all metrics.

In 2009, Shuo Guo et al., [27] proposed Faulty Node Detection (FIND) method for wireless sensor networks. Detecting nodes with fault is a major issue in network management. To overcome this, FIND detects nodes with faulty readings based on their relative sensing results. To detect the node sequences, an approach is proposed to estimate where the events are taken place and what are the original sequences. Secondly, the average ranking differences of nodes in detected sequences and original sequences for faulty nodes are determined. The experimental results proved that the FIND achieved both a low false negative rate and a low false positive rate in various network settings.

In 2009, Elbhiri Brahim et al., [28] presented a Stochastic and Balanced Distributed Energy-Efficient Clustering (SBDEEC) scheme for heterogeneous wireless sensor networks by dividing the network into dynamic clusters. It is a balanced and dynamic method where the cluster head election is more efficient. The method estimates the average energy and selects the algorithm cluster head for broadcasting the sensed information in the searched data; nodes with significant data send its message to the cluster head. From the Results it was observed that SBDEEC is more efficient than SEP and DEEC.

In 2009, Dr.G. Padmavathi et al., [29] presented the summary of attacks and their classifications in wireless sensor networks. The security mechanisms are actually used to detect, prevent and recover from the security attacks. The standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA) are also presented. The secondary goals are also mentioned such as Data Freshness, Self- Organization, Time Synchronization and Secure Localization.

In 2010, Mohammad Saifuland and A.F.M. Sultanul Kabir [30] proposed a hierarchical architect based on intrusion detection system for wireless Ad hoc sensor network. The policy based detection mechanism with GSM cell concept is introduced for intrusion detection architecture. In that mechanism, the cluster nodes are considered as more powerful than ordinary sensor nodes. The result showed that, the proposed scheme increased the total cost of network set up, but enhances reliability, efficiency and effectiveness of IDS for a large geographical area.

In 2011, Yenumula B. reddy et al., [31] proposed an Agent-based Trust Calculation approach to calculate the trust using the collaborative approach. The framework used the characteristic of neighbouring node for calculating the successive node. Authors also presented the fuzzy rating models and Sporas formula for node rating. The clusters formed with the nodes are within communicating distance in the framework. Each cluster has an agent to collect the reputation of nodes. The results showed that the life of a node is increased by using the computational work.

In 2011, Tanveer A. Zia and Albert Y. Zomaya [32] presented a lightweight security framework to provide a comprehensive security solution against the known attacks in sensor networks. The proposed framework consists of four interacting components: a Secure Triple-Key Scheme (STKS), Secure Routing Algorithms (SRAs), a Secure Localization Technique (SLT) and a Malicious Node Detection Mechanism. Additionally, two algorithms (1) sensor node and (2) base station are presented for secure data transfer. Results showed that the effectiveness of the framework ensured the total security by reducing the packet transmission time, latency and packet overheads.

In 2011, Subhankar Mishra et al., [33] described the energy efficient protocols, which can have significant impact on the lifetime of the networks. The algorithm is proposed for minimizing the rate of dissipation of cluster heads. LEAD is combined with energy efficient round scheduling for cluster head allocation. For increasing the lifetime of the networks the cluster heads are selected dynamically in a round schedule balancing scheme. The results exposed that the algorithm perform more energy efficient.

In 2012, Zhenzhong Huang and Jun Zheng [34] proposed a Slepian-Wolf Coding based Energy-Efficient Clustering Algorithm for Data Aggregation in Wireless Sensor Networks. The algorithm, minimize the amount of data generated within each cluster and the overall energy cost for data transmission in the network. In SWEEC algorithm, a sensor node with a larger data compression rate and closer to the sink has a higher probability to

become a cluster head. Simulation results showed that the proposed SWEEC algorithm reduced the overall energy cost for data transmission and improved the energy efficiency of the network.

In 2014, Sivanandam and Kirankumar [35] presented the method of identifying malicious nodes using node classification in wireless sensor network. Three techniques are proposed for providing security in the network such as node monitoring, packet sealing and node classification. In the implementation phase, two algorithms have been proposed to identify the behaviours of sensor nodes. Generally, Directed Graph (DG) establishment and Packet Transmission algorithm are performed for identifying the packet dropping malicious nodes. Further, the node classification algorithm is used to calculate the node dropping ratio and find the status pattern. Simulation results showed that, the proposed scheme is more effective to identify misbehaving forwarders that drop packets.

In 2014, Reshmi and Vidya [36] exposed the contending against energy depletion attack in wireless network. Security is one of the critical issue in networks. To overcome these issues, No-Backtracking property scheme is proposed to achieve high efficiency and secure authentication. The group identification method is used to identify the nearest neighbour node within the network. The PLGP protocol is a state secure routing protocol, which is used to resist vampire attack during packet forwarding. In PLGP, all the nodes are formed as a group or a tree structure to validate the packets for addressing and routing. The results represented that, the PLGP protocol based on no-backtracking property has performed well for depletion of vampire attacks.

In 2014, Menasinakai et al., [37] explained the prevention and detection of vampire attacks. PLGP protocol is used to prevent the vampire attacks. It consists of two phases for forwarding the packets in a tree structure such as topology discovery phase and packet forwarding phase. To securely transmit the data, the path tracking technique is used in PLGP. It demonstrated the routing lead distribution and path diversity. The buffer technique also used in the proposed system in which the details of previous activity of every node is stored in a small buffer.. The simulation results showed that, the proposed scheme is performed well to prevent attacks and achieved high energy consumption.

In 2014, Divya and Vanitha [38] presented a valuable secure protocol to prevent attacks in wireless ad hoc sensor networks. The Valuable Secure Routing Protocol (VSP) is proposed to prevent vampire attacks. It is compressed of three phases such as network configuration phase, key management and communication phase. In first phase, the neighbour group formation process is done by each and every node. The key management phase is used for cryptography to protect the node and data. Elliptic Curve Cryptography (ECC) approach is based on the algebraic structure which is used to achieve the security with smaller key size and minimize the number of calculation in a group. PLGP protocol is used to perform the backtracking method in communication phase.

In 2014, Damodhar and Umakant [39] described the resource consumption attacks in wireless ad hoc sensor networks. The Energy Weighted Monitoring Algorithm is proposed for providing the security in network. Two phases are initialized in EWMA for consuming the nodes energy. Network configuration phase establishes an optimal routing path from source to destination and achieved multi hop load balanced network. Communication phase avoids the same data packets and aggregated the data transmission. Simulation results proved that the proposed scheme performs well.

In 2014, Sivakumar and Murugapriya [40] described the detection and elimination of vampire attacks in sensor networks. Optimal Energy Boostup protocol is proposed for providing the security. The PLGP protocol is performed as a tree structure. It predicts the vampire attacks based on the behaviours of nodes and used to find the optimal path. From the results, it was observed that the network energy is increased based on the location in forwarding phase.

In 2014, Palle and Seelamsaireddy [41] presented a method of detection and elimination of vampire attacks in wireless sensor networks. To overcome the vampire attacks, Optimal Energy Boost up Protocol (OEBP) and Energy Weighted Monitoring Algorithm (EMWA) method are proposed. The goal of EMWA method is to establish an optimal routing path. Further, the PLGP protocol is presented to prevent vampire attacks. Additionally, AODV protocol with small delay and DSDV protocol with RIP method are used to provide the security. The results showed that, the proposed scheme performed better in the effect of network energy.

In 2014, Soramrakeshsingh and Narendra [42] presented the performance of energy attack detection in wireless sensor network. Vampire attacks are very difficult to detect. To overcome this issue, the PLGP and M-DSDV protocol are proposed to detect the resource depletion attack. PLGP attestation phase is the best use of finding the path in the tree structured network. M-DSDV protocol is designed to overcome the routing loop problems. Two phases are clarified in the protocol, topology discovery phase and maintenance phase. The results demonstrated that, the PLGP protocol and DSDV protocol have reduced the damage from vampire attacks.

In 2014, Blessy and Petchimuthu [43] presented a captivating approach for disclosing the vampire intrusion in wireless sensor network. For providing the security in networks, the LEACH algorithm is proposed to increase the lifetime of network. It reduced the data aggregation energy in data transmission. CDMA and TDMA schedules are also used in LEACH protocol to reduce the obstruction between the clusters. The simulation results showed that the proposed schemes improved the lifetime of the networks.

In 2014, José Anand and Sivachandar [44] presented the vampire attacks detection in wireless sensor networks. Ihe effect of vampire attacks on AODV is proposed for providing the security. The vampire attacks have the ability to disrupt the AODV protocol. Randomly selected malicious AODV agents are evaluated. Initial energy and final energy are used to calculate the energy level in the networks. The results proved that the proposed scheme increased the network energy during the forwarding phase.

In 2014, Sharmila and Ramalingam [45] described the energy depletion attacks in wireless sensor networks. The Adaptive Traffic Coalescing (ATC) scheme and Adaptive Power Aware Multicasting (APAM) algorithm are proposed to detect DoS attacks and decrease the energy consumption. ATC monitored the incoming traffic and can detect DDoS attack traffic. The Enhanced On-Demand Distance Vector (ENAODV) routing protocol is used to detect the attacks. The simulation results showed that the ENAODV protocol performed well in high energy level and the ATC method has effectively detected the DDoS attacks.

III. ISSUES

From this literature survey, the following issues are identified in Ad-hoc sensor Networks.

1. It consumes more Energy and time.
2. It constraints low Bandwidth.
3. It produces high error rates and routing attacks.
4. Limited resources, Latency, security problem, Scalability and Integrity.
5. It provides difficulties in coverage area and positioning the network.

IV. CONCLUSION

This paper presents the overview of attacks and detection methods in ad-hoc sensor networks. Performance and evaluation of black hole attack, white hole attack and vampire attacks are also described clearly. Most of the fundamental issues such as More Energy consumption, Less Bandwidth constraint and High error rates, Limited resources, Latency, security problem, Scalability and Integrity are explained and overcoming techniques are also presented for effectiveness of the networks. Further, this survey helps to implement new approaches to prevent the vampire attacks in wireless ad hoc sensor network.

References

[1] Wendi RabinerHeinzelman, AnanthaChandrakasan, and HariBalakrishnan "Energy-Efficient Communication Protocol forWirelessMicrosensor Networks," Proc. IEEE Transactions on, Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[2] SeapahnMeguerdichian, FarinazKoushanfar, Gang Qu, MiodragPotkonjak"ExposureIn Wireless Ad-Hoc Sensor Networks", Wireless Communications and Networking Conference, IEEE WCNC 2001.

[3] AratiManjeshwar and Dharma P. Agrawal" APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks" Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS.02)

[4] Wei Ye, John Heidemann, Deborah Estrin" An Energy-Efficient MAC Protocol for WirelessSensor Networks" in Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, 2002

[5] Rahul C. Shah and Jan M. Rabaey, Energy aware routing for low energy ad hoc sensor networks, Wireless Communications and Networking Conference, IEEE WCNC2002

[6] VaidyanathanRamadurai, Mihail L. Sichitiu, "Simulation-based Analysis of a Localization Algorithm for Wireless Ad-Hoc Sensor Networks*",* in Proceedings of International Conference on Wireless Networks (ICWN), June 23-26, 2003.

[7] RoozbehJafari, FoadDabiri, and MajidSarrafzadeh"On Minimal Energy Skew Routing in Lossy Wireless Sensor Networks*"Journal of Low Power Electronics*, 1(2):97–107, 2003.

[8] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,"Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications, 2003

[9] SeemaBandyopadhyay and Edward J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," Proc. IEEE Transactions on, Wireless Sensor Network, INFOCOM 2003.
[10] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l WorkshopSensor Network Protocols and Applications, 2003.
[11] Haowen Chan Adrian Perrig Dawn Song" Random Key Predistribution Schemes for Sensor Networks"Proc. IEEE Transactions on, Wireless Sensor Network 2003
[12] O. Younis and S.Fahmy"HEED: A Hybrid, Energy Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks," *IEEE Transactions on Mobile Computing*, 3(4):660-669, 2004.
[13] ImadAad ,Jean-Pierre Hubaux and Edward W. Knightly"Denial of Service Resilience in Ad Hoc Networks" Proc. ACM MobiCom, 2004
[14] Timothy J. McNevin, Jung-Min Park, and Randolph Marchany("pTCP: A Client Puzzle Protocol For Defending Against Resource Exhaustion Denial of Service Attacks ") Technical Report TR-ECE-04-10, Department of Electrical and Computer Engineering, Virginia Tech, Oct. 2004
[15] Xiang Ji, HongyuanZha"Sensor Positioning in Wireless Ad-hoc SensorNetworks Using Multidimensional Scaling"In Proceedings of the 12th International Conference onComputer Communications and Networks, pp.527-532,2003
[16] Stefan Schmidt and HolgerKrahnSecurityArchitecture for Mobile Wireless Sensor NetworksFirst European Workshop (ESAS 2004) Heidelberg, Germany, August 6, 2004
[17] Haibin Sun John C.S. Lui"Distributed Mechanism in Detecting and Defending Against the Low-rate TCP Attack"International Conference of Network Protocols (ICNP) 2006, Berlin, Germany
[18] Yih-Chun Huand Adrian Perrig, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wireless Networks 11, 21–38, 2005
[19] Li Qing, Qingxin Zhu, Mingwen Wang" Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks"Computer Communications 29 (2005) 2230–2237
[20] Ping Ding, JoAnne Holliday, AslihanCelik"Distributed Energy-Efficient Hierarchical Clustering for Wireless Sensor Networks" Wireless Sensor Networks 14, 2005 ref10
[21] Jing Deng, Richard Han and Shiva Kant Mishra ("Limiting DoS attacks during multi hop data delivery In wireless sensor networks")Int. J. Security and Networks, Vol. 1, Nos. 3/4, 2006
[22] Sencun Zhu, ShouhuaiXu, SanjeevSetiaandSushilJajodia "LHAP: A Lightweight Network Access Control Protocol for Ad-Hoc Networks" Computer Communications 49 (2006)
[23] MujdatSoyturk and TurgayAltilar" A Routing Algorithm for Mobile Multiple Sinks in Large-Scale Wireless Sensor Networks"Wireless Pervasive Computing, 2007.
[24] Vahid Shah-Mansouri and Vincent W.S. Wong" Distributed Maximum Lifetime Routing in Wireless Sensor Networks Based on Regularization"Proc. IEEE Transactions on, Ad-hoc and Sensor Networking Symposium, 2007
[25] BuyanjargalOtgonchimeg and Youngmi Kwon" EECED: Energy Efficient Clustering Algorithm for Event-Driven Wireless Sensor Networks" Joint Conference on INC, IMS 2009
[26] Allan I. McInnes" Model-checking the Flooding Time Synchronization Protocol" IEEE International Conference on Control and Automation Christchurch, New Zealand, 2009.
[27] ShuoGuo, ZiguoZhong and Tian He" FIND: Faulty Node Detection for Wireless Sensor Networks", Proc. ACMWorkshopSecurity of Ad Hoc and Sensor Networks, 2009
[28] ElbhiriBrahim, SaadaneRachid, Alba-Pagès Zamora, DrissAboutajdine "Stochastic and Balanced Distributed Energy-Efficient Clustering (SBDEEC) for heterogeneous wireless sensor networks" Joint Conference on INC, IMS 2009

[29] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, " A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks"(IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

[30] Mohammad Saiful Islam Mamun" Hierarchical Design Based IntrusionDetection system for Wireless Ad Hoc Sensor Network" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[31] Yenumula B. Reddy and RastkoSelmic" Agent-based Trust Calculation in Wireless Sensor Networks"SENSORCOMM 2011: The Fifth International Conference on Sensor Technologies and Applications

[32] Tanveer A. Zia,Albert Y. Zomaya "A Lightweight Security Framework forWireless Sensor Networks" Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 3, pp. 53-73 2011

[33] Subhankar Mishra, Sudhansu Mohan Satpathy and Abhipsa Mishra "Energy Efficiency In Ad Hoc Networks " International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.1, 2011

[34] Zhenzhong Huang and Jun Zheng "A Slepian-Wolf Coding based Energy-Efficient
Clustering Algorithm for Data Aggregation in Wireless Sensor Networks" IEEE ICC 2012 - Ad-hoc and Sensor Networking Symposium

[35] S.Sivanantham, K.Kirankumar, G.Saravanagokul," Identifying Malicious Nodes in Wireless Sensor Networks using Node Classification" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 9, 2013

[36] Vidya.MReshmi.S "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks" International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1, Issue 1 2014

[37] SoumyashreeMenasinakai, Shanthi.M.B, Dr.Dinesh.K.Anvekar "Prevention and Detection of Vampire Attacks Problem in Wireless Ad-Hoc Sensor Network" In Proc. International Conference on Information and Communications Security Protocols, 2014.

[38] K.Vanitha,V.Dhivya" A Valuable Secure Protocol to Prevent Vampire Attacks in Wireless Ad Hoc Sensor Networks" International Journal of Innovative Research in Science, Engineering and TechnologyVolume 3, Special Issue 3, 2014

[39] B. Umakanth, J. Damodhar "Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks" international Journal of Engineering Research Volume No.3 Issue No: Special 2, pp: 107-111, 2014

[40] K.Sivakumar, P.Murugapriya " Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks " International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, 2014

[41] Monica Palle, SeelamSaiSatyanarayana Reddy "Detection Elimination and Overcoming of Vampire Attacks in Wireless Ad hoc Networks " IJRIT International Journal of Research in Information Technology, Volume 2, Issue 6, 2014, Pg: 224-237

[42] SoramRakesh Singh, NarendraBabu C R " improving the performance of energy attack detection in wireless sensor network by secure forwarding mechanism " International Journal of Scientific and Research Publications, Volume 4, Issue 7, 2014

[43]S.BlessyVedhaP.Petchimuthu "A Captivating Approach for Disclosing Vampire Intrusion in WSN" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, 2014

[44] Jose Anand, K. Sivachanda "Vampire Attack Detection in Wireless Sensor Network " International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, 2014
[45] V.Sharmila, Mr. K. MuthuRamalingam "Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network" International Journal of Computer Science and Mobile Computing Vol. 3, Issue. 8, 2014, pg.100 – 109

