Detection and Prevention Schemes in Mobile Ad hoc Networks

Jeelani[1], Subodh Kumar Sharma[2], Pankaj Kumar Varshney[3]

[1]Scholar, Mangalayatan University, Aligarh, India
[2]Associate Professor, Mangalayatan University Aligarh, India
[3]Associate Professor, Department of Computer Science, IITM Janakpuri, New Delhi, India
jeelani.jee@gmail.com, Subodh.sharma@mangalayatan.edu.in
pankaj.surir@gmail.com,

Abstract- Wireless Sensor Network (WSN) has wide range of application areas such as health care, military and industry for real time event detection. The sensing capability of a Wireless Sensor Network (WSN) requires sensor node as a network of it. But these nodes are constrained in terms of size, energy, memory, processing power. These nodes sense environmental data perform limited processing and communicate over short distances. As the applications of wireless sensor networks are continuously growing also the need for security mechanisms is increasing day by day. It is very essential to save WSNs from malevolent attacks in unfriendly situations. Such systems require security design because of different restrictions of assets and the noticeable attributes of a remote sensor arrange which is a impressive test. This article is a broad survey about issues of WSNs security, which inspected as of late by analysts and a superior comprehension of future bearings for WSN security.

Keywords- Mobile Ad hoc Network, Wireless Sensor Network, Denial of service.

I. INTRODUCTION

Wireless sensor networks as a part of MANET consist of large number of tiny sensor nodes that continuously monitors environmental conditions. Wireless Sensor Networks are a collection of thousands of sensor nodes that are self-organized and are capable of wireless communication. But these nodes are constrained in terms of size, energy, memory, processing power [23]. These nodes sense environmental data perform limited processing and communicate over short distances. As the applications of wireless sensor networks are continuously growing also the need for security mechanisms is increasing day by day. Wireless Sensor Networks may interact with sensitive data or usually these networks operate in hostile, unattended environments, it is necessary to address these security concerns. Security challenges of sensor networks are different from traditional networks due to many constraints of these networks. Moreover when we look at the applications of WSNs, there are many applications areas, e.g., battlefield awareness, traffic monitoring system etc. In which security of information remains as an important issue. Providing security to a WSN is a nontrivial problem. Security mechanisms which are applicable to wired or other ad-hoc networks are not suitable for WSN. There are many reasons behind it and we discuss those in the subsequent sections. Though there are varieties of challenges in sensor networks, here we focus on different security issues and possible remedies of those.

A. Security Requirements in Wireless Sensor Networks

The main security requirements that each WSN has to fulfill are as follows.

Confidentiality: Secrecy of message transmitted between nodes should be maintained properly. For that important segments of message should be encrypted. In some cases even the two end points are also hidden. In some dynamic systems where nodes keep on joining and leaving the network, forward and backward secrecy needs to be maintained. Forward Secrecy means that nodes leaving the network may not be able to access future transmissions on the network after leaving the network and Backward Secrecy means that new nodes may not be able to access past transmissions before their joining the network. These phenomenons are needed to maintain confidentiality of data in wireless sensor networks [23].

Authenticity: For preparation the security of communicating node's identities, authenticity is vital. Any node must verify even if an accepted message comes from a true sender. In the absence of authentication, attackers without difficulty are able to extend wrong data into the wireless sensor networks. Generally, for authentication the origin of a message, an annexed message authentication code possibly employed [22].

Integrity: Integrity should be prepared to assure that attackers cannot change the transmitted messages. Attackers are able to establish interference packets to modify their polarities. In addition before forwarding them a malicious routing node can alter significant data in packets. To find random errors throughout packet transmissions as a cyclic redundancy checksum (CRC) employed for detecting them, similarly keyed checksum, for example a MAC use to secure packets against changes [22].

Availability: WSN services should always be available in spite of all the resource depletion attacks that may occur on the system. So our network should be resistant to such attacks [23].

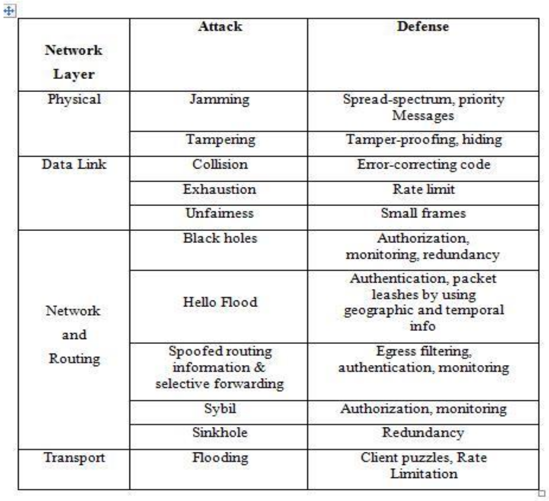
Non-Repudiation: Neither the sender nor the receiver should be able to deny that the message is sent by him. For that message can be digitally signed by both the sender and the receive [23].

B. Attacks on Wireless Sensor Networks

Since wireless sensor networks operate in unsafe environment these are vulnerable to several types of attacks.

Denial of service attack: Denial-of-Service attack is the serious attack as it consumes the network resources like energy, bandwidth and power. Denial of service attack floods access amount of unnecessary packets in the network and affects the overall performance of the network. If there is only single attacker in the network then this is DoS attack and if there are multiple attackers then this is known as Distributed Denial of Service (DDoS) attack. Denial of service attack is multilayer attack. In WSN there are numerous DOS attacks on different layers like jamming, tampering, exhaustion, flooding and so on [3].

DENIAL-OF-SERVICE DEFENSE IN WSNs [22]



Network Layer	Attack	Defense
Physical	Jamming	Spread-spectrum, priority Messages
	Tampering	Tamper-proofing, hiding
Data Link	Collision	Error-correcting code
	Exhaustion	Rate limit
	Unfairness	Small frames
Network and Routing	Black holes	Authorization, monitoring, redundancy
	Hello Flood	Authentication, packet leashes by using geographic and temporal info
	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sybil	Authorization, monitoring
	Sinkhole	Redundancy
Transport	Flooding	Client puzzles, Rate Limitation

Hello Flood attack: HELLO flood attack is one of the active attacks that flood the HELLO packets in the network. In wireless sensor network attacker transmit the packets from source node to destination publicizing the packets as cluster head. All sensor nodes will select these packets and send join packet into it, thinking that the attacker is their neighbor and the entire network will be in confusion. In wireless sensor network the sensor nodes are deploy in normal orchestrated region. And the data is transmitted from source node to destination through intermediate nodes. Sensor nodes does not distinguish that the enemy node is not their neighbour nodes. So as a result network is spoofed by the attacker [3].

Attacks on Information during transmission: The most dangerous attack in WSN are on information that is being transmitted between nodes because that information is susceptible to eavesdropping, injection, modification.

Traffic analysis attack can also be performed because attacker may be able to get to know about the layout of the network and can damage the busiest portions of the network to perform greatest damage [23].

Replicating a Node Attack: The attacker may insert a new node into the sensor network which can be a clone to an pre-existing node. This new cloned node can transmit useful information to the attacker. This node replication attack is most dangerous when the cloned node is some base station. So base stations needs to be deployed in secure locations [23].

C. Routing Attack

The attacks that affect the routing protocol of wireless sensor network are as follows:

Selective Forwarding: In Selective Forwarding attack the malicious node may drop certain packets and transmit the rest. If it drops all the packets then it is a Black Hole attack. But if it forwards selective packets then is selective forwarding attack. The effectiveness of the attack depends on how close is the malicious node to the base station because then maximum traffic will go through it [23].

Sinkhole Attacks: Sinkhole Attack is to attract maximum traffic through malicious node which is placed somewhere near the base station. If the sensor network has one main base station then this attack can be dangerous [23].

Sybil attack: In Sybil attack one node presents multiple identities in the network that may mislead nodes in the network. Sybil attacks can be used against topology maintenance and routing algorithms [23].

Wormhole Attack: In Wormhole attack just like Sinkhole attack the attacker sitting closer to base station may tunnel the traffic to a low-latency link thus disrupting the traffic [23].

II. LITREATURE REVIEW

The present literature review is based on the research work entitled “Security attacks detection and prevention schemes in wireless sensor networks”. For reviewing of literature, the researcher has gathered more of articles as a secondary source of data from which, selected material or articles related to the researcher topic in order to acquire depth knowledge on the related topic and completed in the past days. After reviewing of previous research articles, the researcher summarized the reviewed literature and to end up with, a research gap has been introduced.

Guechari, M et al.[1] presented an experimental study on dynamic approach for detecting Denial of Service (DoS) attacks in cluster-based sensor networks. That method is based on the election of controller nodes called cNodes which observe and report DoS attack activities. Each cluster contains cNodes and normal sensor nodes. The role of a cNode is to analyze traffic and to send back a warning to the cluster head if any abnormal traffic is detected.The election of these cNodes is dynamic, and done periodically and based on a Multiplicative Linear-Congruential Generator (MLCG).

Rolla P. and Kuar M.[2] concluded an experimental study on time allocation based request forwarding window technique to detect and prevent DoS (Denial of Service) attack. DoS attacks are flooding access amount of packets in the network that consumes the energy of the network. In Profile based Protection Scheme (PPS), the behavior of all the nodes deployed in the network are observed.

Patil S. and Choudhari S.[3] analyzed that Denial-of-Service (DoS) attack is most popular attack in sensor network. Attack prevention techniques such as fuzzy Q-learning algorithm, Dynamic Source Routing (UDSR), Secure Auction-based Routing (SAR), have been used by author against DoS attacks. They proposed cooperative immune system is an enhancement to the existing immune system, CO-FAIS, which will improve the accuracy of the system. In the stands they have reduced the false alarm rate.

Naik S. and Shekokar N.[4] designed and experimental program on defending the mechanism against the denial of sleep attack. This solution is an effective method for preventing this attack as all the nodes sending the synchronization messages will be validated before those messages are accepted and rejected if the node is not validated. The attacker node cannot replay the sleep synchronization signal again as its sleep schedule will not be accepted without authentication.

Chaudhary S. and Thanvi P.[5] concluded an experimental study on modified variant of Ad-hoc On Demand Distance Vector (AODV) protocol to analyze the effect of Dos attack on system performance and later apply the prevention scheme to analyze the change in network performance. Researcher have used scenario in an experimental which are Topology scenario for 80 nodes, simulation in progress, average End-to-End Delay, Throughput analysis, Packet ratio and Packet drop analysis. For successful attack detection various methods have been proposed over time. The technique used by researcher based on comparison on RREP sequence number of packet received by the sender from its neighbors broadcasting the availability of fresher or shorter routes.

S. Fouchal et al.[6] carried out a parametric study to a novel approach to detect denial attacks in Wireless Sensor Networks. This is approach based on a recursive clustering. They have approved our proposition with two clustering algorithms on 100-sensor networks. In fact, they used the LEACH (low energy algorithm adaptive clustering hierarchy)and FFUCA (Fast and flexible unsupervised clustering algorithm) algorithms. The results are convincing in terms of the detection of the groups. In addition, the use of FFUCA induces a better management of energy and thus a longer network lifetime.

Mansouri D et al.[7] presented study on a method for detecting and preventing Denial of Service attacks in WSNs. The detection method they have considered is based on using special control nodes which are monitoring the throughput of traffic in clusters. Control nodes (Cluster Heads) are elected by using recursively LEACH clustering algorithm. We have presented by means of a set of experimentation, using Simevents simulator. The numerical results obtained show that our approach gives significant results in term of detection rate and time detection.

Kiss I., Haller P. and Beres A.[8] proposed a clustering based approach for detecting the influences of cyber-attacks, especially those of denial of service (DoS) attacks, in the observed of the system. Proposed approach is presented in contrast with TEP (Tennessee Eastman challenge process) therefore several scenario of DoS attack are experimented to validate the effectiveness of the method. Researcher have used the SCADA (Supervisory Control And Data Acquisition) simulator this approach.

Ballarini P., Mokdad L. and Monnennt Q.[9] proposed a dynamic cNodes displacement schema according to which cNodes are periodically elected among ordinary nodes of each atomic cluster. Such a solution results in a better energy balance while maintaining good detection coverage. They analyze the tradeoffs between static and dynamic solutions by means of two complementary approaches: through simulation with the NS-2 simulation platform and by means of statistical model checking with the Hybrid Automata Stochastic Logic. Researcher have used different different models which are Non-Markoveianmodling and verification of DoS, Generalized stochastic Petri nets (GSPN), eGSPN and HASL modeling checking with two algorithm which are LEACH and k-LEACH.

Ghildiyal S et al.[10] focued on the Wireless Sensor Network characteristics, constraints and types of DoS attacks at different layer. Different layers of WSN nodes have variety of roles to play for proper their proper functioning at different layers like signaling, framing, forwarding, reliable transportation and user interaction at both receiving as well as sending end. Many denial of service attacks are identified at each layer which are meant for purposeful, planned attacks to jeopardize the availability of service, restricting the WSN utility for application.

Wazid M et al.[11] carried out a parametric study of Blackhole attack is measured on the network parameters followed by the proposal of a novel technique for the detection and prevention of Blackhole attack in WSN. The presences of blackhole attack both parameters of network which are End-to-end delay and Throughput are affected. They have observed that in the presence of blackhole attack the performance of network degraded very rapidly. The End-to-end delay increases to 4.03 msec and throughput decreases to 5027.85 bps. So it has become very important to provide a detection and prevention mechanism for blackhole attack.

Singh V. Pal, UkeyAnand A. S. and Jain S.[12] proposed to detect and prevent hello flood attack using signal strength of received Hello messages. Nodes have been classified as friend and stranger based on the signal strength of Hello messages sent by them. Nodes classified as stranger are further validated by sending a simple test packet; if the reply of test packet comes back in a predefined time then it is treated as valid otherwise it is treated as malicious. The algorithm is implemented in ns-2 by modifying the AODV-routing protocol. The performance of algorithm has been tested under different network scenarios. The simulation results show improved performance of the new algorithm in terms of number of packet delivery ratio as compare to AODV with hello flood attack, hello flood attack is an important attack on the network layer, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node using high transmission power and break the security of WSNs.

Hai T. H. and Eui-Nam H.[13] proposed a lightweight detection algorithm based only on the neighborhood information. His detection algorithm can detect selective forwarding attack with high accuracy and little overhead imposed on detection modules than previous works. His algorithm has been evaluated and shows a good effectiveness even the high density of network and the high probability of collisions in WSNs. Besides, our detection modules consume less energy than previous works by using over-hearing mechanism to reduce the transmission of alert packets.

Malik R. and Sehrawat H.[14] studied on some important attacks over WSNs with possible ways to detect and defend selective forwarding attack. WSNs have issues like low memory and limited battery availability, so conventional security establishments are not effective here. A number of attacks are possible over WSNs like black hole, wormhole and selective forwarding attack. Selective forwarding attack is a special case of black hole attack where compromised nodes drop packets selectively. Researcher have reviewed the some OSI layers such as Application, Transport, Network, Data link and Physical and these attacks and defense strategy.

Soni V., Modi P. and Chuadhri V.[15] have presented some countermeasures against the sinkhole attack. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as black hole or gray hole. Ultimately this drop of some important data packets can disrupt the sensor networks completely.

Rassam M. A et al.[16] concluded that the vulnerabilities of Mintroute protocol to sinkhole attacks are discussed and the existing manual rules used for detection are investigated using different architecture. On here different types of protocols were proposed for WSN, they cannot guarantee the protection of the network from different attacks. Sinkhole attacks which are launched by a new or a compromised node attracts the network traffic to pass through it. This attack leads to many other attacks such as blackhole, wormhole, or even information fabrication attacks.

Khanderiya M. and Panchal M.[17] proposed work researcher has tried to give a method that could detect Sybil attack in Wireless Sensor Networks. Researchers have developed many schemes and methodologies for detecting and preventing Sybil attack, but these security mechanisms are not being used satisfactorily in real scenario for Wireless Sensor Networks. They have presented a robust and lightweight solution to detect Sybil attack using RSSI (Received Signal strength Indicator). RSSI value is used for detecting Sybil attack, but there three detectors were used for this scheme. Three detectors were required because the nodes that are at same distance from detecting node would have same RSSI value, so single node was not enough for detection process, as it would regard those nodes as Sybil too.

Dhamodharan U. K. R. and Vayanaperumal R.[18] designed and experimental program on a scheme of assuring security for wireless sensor network, to deal with attacks of these kinds in unicasting andmulticasting. Basically a Sybil attack means a node which pretends its identity to other nodes. Communication to an illegal node results in data loss and becomes dangerous in the network.The existing method Random Password Comparison has only a scheme which just verifies the node identities by analyzing the neighbors. A survey was done on a Sybil attack with the objective of resolving this problem.The survey has proposed a combined

CAM-PVM(compare and match-position verification method) with MAP (message authentication and passing) for detecting, eliminating, and eventually preventing the entry of Sybil nodes in the wireless sensor networks.

Amish P. and Vaghela V. B.[19] carried out a parametric study on the techniques dealing with wormhole attack in WSN are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. As compared to other solution shown in literature, proposed approach looks very promising. NS2 simulator is used to perform all simulation.

Shaikh F. A. and Patil U.[20] carried out the study to explain a wormhole detection algorithm for Wireless Mesh Networks which detect the wormholes by calculating neighbor list as well as directional neighbor list of the source node. The main aim of the algorithm is that it can offer approximate location of nodes and effect of wormhole attack on all nodes which is helpful in implementing countermeasures. The performance evaluation is complete in varying no. of wormholes in the network.

Modirkhazeni A. et al.[21] carried out the parametric study to focused on wormhole attack and proposed distributed network discovery approach to mitigate its effect. Researcher has presented selected countermeasures and then we proposed network discovery approach which needs no additional tools or accurate time synchronization. According to the simulation our approach can mitigated almost 100% of wormhole attack overload in the environment where 54% of nodes are affected with the wormhole.

Ahmad Salehi S. et. al.[22] have analyzed networks require security plan due to various limitations of resources and the prominent characteristics of a wireless sensor network which is a considerable challenge in WSNs the node nature causes limitations like restricted energy, capability of processing, and storage capacity. These restrictions create WSNs so distinctive from conventional ad hoc wireless networks. Specific methods and protocols have been advanced to utilize in WSNs. All of the mentioned security dangers including the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, offer one usual goal which is for compromising the integrity of the network they attack. In this paper, they principally concentrate on the threats in WSN security and the abstract of the WSNs threats which influence various layers along with their defense techniques is presented.

Bhalla M., Pandey N. and Kumar B.[23] have analyzed security issues and vulnerabilities in wireless sensor networks. All the security protocols mentioned should be analyzed using simulation and some more features like speed-of- operation, Power Consumption and Efficiency should be evaluated.

Aldhobaiban D., Elleithy K. and Almazaydeh L.[24] carried out an experimental research has shown how the network nodes can be rerouted to avoid the attacked nodes. The deletion of the links for the infected node and its neighbor leads to the security of the rest of the node network. Since this approach requires a table to monitor all the nodes, the load on the network is overwhelming.

Sakthivel T. and Chandrasekaran R. M.[25] carried out the proposed Path Tracing (PT) algorithm for detection and prevention of wormhole attack as an extension of DSR protocol. The PT algorithm runs on each node in a path during the DSR route discovery process. The PT algorithm detects and prevents the wormhole attack using per hop distance between two nodes. They proposed algorithm implementation depends on DSR protocol. They then simulated the proposed algorithm in NS-2. The parameters like throughput, overhead and the average delay of the proposed algorithm are compared with that of existing wormhole prevention techniques.

Modirkhazeni A et al.[26] focused on wormhole attack and proposed distributed network discovery approach to mitigate its effect.Then they focused on the wormhole attack in these kinds of networks and presented selected countermeasures. Afterward they generalized previous countermeasures, analyzed them and selected the better one. And then base on the presented results they proposed network discovery approach base on distributed scheme which needs no additional tools or accurate time synchronization. According to the simulation proposed approach acted efficiently and mitigated almost 100% of wormhole attack overload in the environment where 54% of nodes are affected with the wormhole.

S. I. Eludiora, et.al[27] reviewed the existing approach to security solutions in WSNs and proposed the use of a distributed approach. The approach will allow SNs to communicate directly with the BSs rather than forming cluster-heads among themselves. Mobile Agents (MAs) were introduced to facilitate communication among the BSs. MAs can easily move from one host to another and perform necessary tasks. Researchers developed a Distributed

IDS for WSNs. Distributed IDS is implemented using TMote sky wireless sensor for testing and simulation over specified parameters.

Ioannou C., Vassiliou V. and Sergiou C[28] have analyzed they proposed a general methodology of an anomaly-based Intrusion Detection System (IDS), named mIDS, that uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activity to either benign or malicious to detect a malicious behavior within a sensor node. Attacks have been implemented within the Contiki O/S and we tested the results using the associated COOJA simulator. All sensor nodes are equivalent to TelosB nodes and have a 25m radio range. They created a model that took into consideration both attacks and evaluated in different network topologies.

Shanthi. S., E. G, Rajan[29] discussed many potential issues of WSN security and detection mechanisms and present a comprehensive analysis of various Intrusion Detection approaches (signature based detection system, anomaly based detection system, hybrid based detection system) in Wireless Sensor Networks.

III. CONCLUSION

The interest for security in WSNs turns out to be more self-evident amid capacity development of WSNs and they are utilized substantially more, nonetheless, in WSNs the hub nature causes impediments like confined vitality, ability of preparing, and capacity limit. These confinements make WSNs so particular from regular specially appointed remote systems. Particular techniques and conventions have been progressed to use in WSNs. The majority of the said security perils including the Welcome surge assault, wormhole assault, Sybil assault, sinkhole assault, offer one common objective which is for trading off the uprightness of the system they assault.

The security of WSNs has turned into a noteworthy subject since of the distinctive perils showing up and the importance of information classification, in spite of the fact that before, there was a little focus on WSNs security. There are a few answers for secure against all risks, albeit a few arrangements have already been recommended. In this article, we essentially focus on the dangers in WSN security and the conceptual of the WSNs dangers which impact different layers alongside their protection methods is displayed. As of late, set up of concentrating on different layers, researchers are striving for incorporated framework for security component. The most normal security risk in different layers and the most sensible arrangement in this paper are exhibited.

REFERENCES

[1] MalekGuechari, Lynda Mokdad and Sovanna Tan. "Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks" IEEE, pp. 173-177, (2012).

[2] Rolla P. and Kuar M.,"Dynamic Forwarding Window Technique against DoS Attack in WSN" IEEE, pp.212-216, DOI 10.1109/ICMETE.2016.93, (2016).

[3] Patil S. and Choudhari S. "DoS attack prevention technique in Wireless Sensor Networks" IEEE, pp.715-721, DOI: 10.1016/j.procs.2016.03.094, (2016).

[4] Naik S. and Shekokar N., "Conservation of energy in wireless sensor network by preventing denial of sleep attack" ELSVIER, PP.370-379, doi: 10.1016/j.procs.2015.03.164, (2015).

[5] Chaudhary S. and Thanvi P., "Performance Analysis of Modified AODV Protocol in Context of Denial of Service (Dos) Attack in Wireless Sensor Networks" International Journal of Engineering Research and General Science Volume 3, pp.486-491(2015).

[6] S. Fouchal et al., "Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks" International journal of communication systems, pp.309-324, DOI: 10.1002/dac.2670, (2015).

[7] Mansouri D., Mokddad L., Ben-othman J. and Ioualalen M., "Preventing Denial of Service Attacks in WirelessSensor Networks" IEEE, PP.3014-3019, (2015).

[8] Kiss I., Haller P. and Beres A., " Denial of Service attack detection in case of Tennessee Eastman challenge process" ELSEVIER, pp.835-841, doi: 10.1016/j.protcy.2015.02.120, (2015).

[9] Ballarini P., Mokdad L. and Monnennt Q., "Modeling tools for detecting DoS attacks in WSNs" Security and Communication Networks, pp.420-436, DOI: 10.1002/sec.630, (2013).

[10] Ghildiyal S., Mishra A. K., Gupta A. and Garg N., "ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS" IJRET: International Journal of Research in Engineering and Technology, pp.140-143, (2014).

[11] Wazid M., Katal A., Sachan R. S., R H Goudar and D P Singh., "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network" IEEE, pp.576-581, (2013).

[12] Singh V. Pal, UkeyAnand A. S. and Jain S., "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks" International Journal of Computer Applications, pp.1-6, DOI: 10.5120/10153-4987, (2013).

[13] Hai T. H. and Eui-Nam H., "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge" IEEE, pp.325-331, DOI 10.1109/NCA.2008.13, (2008).

[14] Malik R. and Sehrawat H., "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks" International Journal of Advanced Research in Computer Science, vol.8, pp.1835-1838, (2017).

[15] Soni V., Modi P. and Chuadhri V., "Detecting Sinkhole Attack in Wireless Sensor Network" International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 2, pp.29-32, (2013).

[16] Rassam M. A., Zainal A., Maarof A. and Al-Shaboti M., "A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks" IEEE, pp.71-75, DOI: 10.1109/ISTT.2012.6481568, (2012).

[17] Khanderiya M. and Panchal M.,"A Novel Approach for Detection of Sybil Attack in Wireless Sensor Networks" IJSRSET, Vol. 2, pp.113-117, (2016),.

[18] Dhamodharan U. K. R. and Vayanaperumal R., "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method" Hindawi Publishing Corporation Scientific World Journal, pp.1-7, http://dx.doi.org/10.1155/2015/841267, (2015).

[19] Amish P. and Vaghela V. B., "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol" ELSEVIER, pp.700-707, doi: 10.1016/j.procs.2016.03.092, (2016).

[20] Shaikh F. A. and Patil U. "Efficient Detection and prevention of Wormhole Attacks in

[21] Wireless Mesh Network" International Research Journal of Engineering and Technology (IRJET), Vol. 4, pp.2208-2214, (2017),.

[22] Modirkhazeni A., Aghamahmoodi S., Modirkhazeni A. and Niknejad N., "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" IEEE, pp.122-128, (2012).

[23] Ahmad Salehi S., Razzaque M. A., Naraei P. and Farrokhtala A., "Security in Wireless Sensor Networks: Issues and Challanges" IEEE, (2013).

[24] Bhalla M., Pandey N. and Kumar B. “Security Protocols for Wireless Sensor Networks” IEEE, pp. 1005-1009, (2015),.

[25] Aldhobaiban D., Elleithy K. and Almazaydeh L., "Prevention of Wormhole Attacks in Wireless Sensor Networks" IEEE, pp.287-291, DOI 10.1109/AIMS.2014.57, (2014).

[26] Sakthivel T. and Chandrasekaran R. M., "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing

Approach" European Journal of Scientific Research, pp.240-252, (2012).

[27] Modirkhazeni A., Aghamahmoodi S., Modirkhazeni A. and Modirkhazeni N., "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" IEEE, pp.122-128, (2012).

[28] S. I. Eludiora, O.O. Abiona, A. O. Oluwatope, S. A. Bello, M.L Sanni, , D. O. Ayanda, C.E Onime E. R. Adagunodo and L.O. Kehinde "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks" IEEE, 2011.

[29] Ioannou C., Vassiliou V. and Sergiou C., "An Intrusion Detection System for Wireless Sensor Networks" IEEE. 2017.

[30] Shanthi. S., E. G, Rajan. "Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks" IEEE 2016, pp. 24-31, 2016