Jurnal
Teknologi

Full Paper

WIRELESS SENSOR NETWORK PERFORMANCE ANALYSIS AND EFFECT OF BLACKHOLE AND SINKHOLE ATTACKS

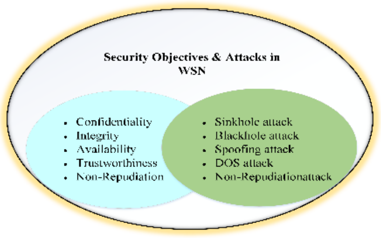
Raja Waseem Anwar*, Majid Bakhtiari, Anazida Zainal, Kashif Naseer Qureshi

Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia.

Article history
Received
25 October 2015
Received in revised form
14 December 2015
Accepted
9 February 2016

*Corresponding author
rajawaseem@gmail.com

Graphical abstract



Abstract

The widespread usage of Wireless sensor networks in various fields and application make it vulnerable to variety of security threats and attacks. These security attacks occur when an adversary compromised a sensor node by inject false measurements and divert real time network traffic. Sinkhole and Blackhole attacks are very common attacks in network, where an attacker advertises un-authorized routing update in network. To deal with these types of attacks, there is a need to tighten the network security and prevent from attackers. In this study, we discuss security threats and presents the effects of Black and Sink hole attacks. Further, the study presents related work and current issues in wireless sensor network. The simulation results illustrated that, how these attacks affect the network performance.

Keywords: WSN; security; black hole; attacks

1.0 INTRODUCTION

The rapid development and advancement in information and communication technologies introduced a tremendous Wireless Sensor Networks (WSNs), which are made up of tiny and low cost sensors with limited processing and computing capabilities. These spatially scattered sensor nodes can measure various types of information from the environment and can make response to events. The Ad-hoc and infrastructure free deployment nature of WSN make it easy to use for various purposes such as military, health, environment monitoring, emergency disaster relief and scientific data gathering [1-3]. In WSN network, various different types of sensor nodes are communicating with each other through multi-hop wireless network. Furthermore, sensors consists of three sub-systems to perform the different tasks like, processing subsystem performs local data computation and processing, the main task of communication subsystem is to exchange the sensed data with its neighboring sensors. Finally the sense subsystem senses the phenomena where it is deployed [4, 5]. Often the collected data is an easy target for adversaries to perform Denial-of-Services (DoS) attack since the collected data is disseminated through insecure medium or channel, however, in order to prevent from these attacks network requires a secure system in WSN.

The remaining paper is organized as follows. The brief overview about the necessary security requirements are presented in Section 2. Section 3 and 4 present the sink and black hole attacks. The simulation results are presented in Section 5 and also discussed the effect of these attacks on network.

2.0 SECURITY REQUIREMENTS FOR WSNS

Usually, the sensor nodes are organized with unattended manner to monitor and collect the data which causes many security threats to Wireless Sensor Networks (WSNs). Data Confidentiality, Integrity and

Availability are major concerns and hence must be considered before the deployment of such kind of networks. Data Integrity measures the trustworthiness of the information provided by the sensor network, the quality of information received which helps in making decision. Similarly Data Confidentiality addresses the need to ensure that collected data from the sensor network will not be available to un-authorized users. Several cryptographic based security approaches have been proposed, which are based on symmetric encryption to preserve data confidentiality [6, 7]. In these encryption based schemes, the public keys are encrypted and the distribution of keys extremely robust [8, 9]. Due to dynamic nature of WSNs, sometime it is so difficult to deploy pre-installed shared keys among node and with base station [10]. Various approaches have been presented to secure WSNs, and protect from attackers (RW Anwar, 2015). Some approaches are based on central access control and some are use extra communication for every message. In WSNs, every node should be self-organize and healing capabilities in order to secure network from attackers.

Secure node localization is another equally vital requirement for WSNs, because it is important to locate sensor nodes automatically and accurately, therefore there is a need to find and rectify the network faults. In WSN, the adversary node creates inaccurate location information by displaying wrong signal strength and replaying messages. To address this issue, a Verifiable multi-literation (VM) was proposed in [7] to ensure location consistency. In VM, two methods are used to find exact and accurate location: authentication ranging and distance bounding. Data authentication considered as another important security requirement in WSN for receiver to verify that the data really originates from the claimed sender. All these requirements are essential to secure WSNs. Figure, 1 shows the important security objectives and attacks in WSN.

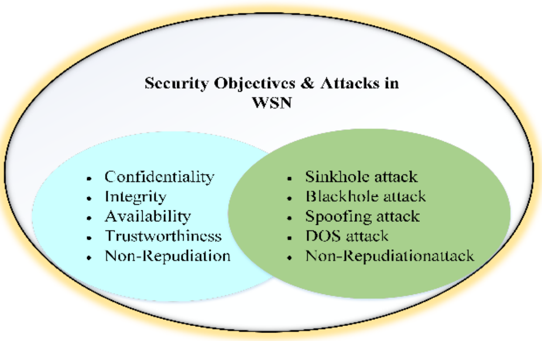


Figure 1 Security objectives and attacks in WSN

Brief descriptions of these attacks are as follows:

3.0 SINKHOLE ATTACK

This type of attack occurs at network layer, in which an adversary attempts to attract all the network traffic from a particular area and preventing the base station from receiving the data from other nodes [11]. Moreover, by including false routing information into compromised node an attacker launch other attacks such as Sybil attack. Subsequently the compromised sensor node reject to forward messages and drop them [12]. The WSN network supports multiple communication patterns, where numbers of nodes send data at a time to one base station, this type of situation is favorable for sinkhole attacks. Furthermore, sinkhole attack does not attack on all sensor nodes, it only attack on that node which is near with base station. The Figure 2a shows the WSN network before or after sinkhole attacks, where node 3 can communicating with base station through node 2 and considered as a shortest route in network. On the other hand, in Figure 2b shows the sinkhole attack, where node 1 compromised and broadcast false information. The false information is about wrong shortest route to base station and other sensor nodes. In addition, the sensor node 3 is communicating by node 1 and leads to false route propagation.

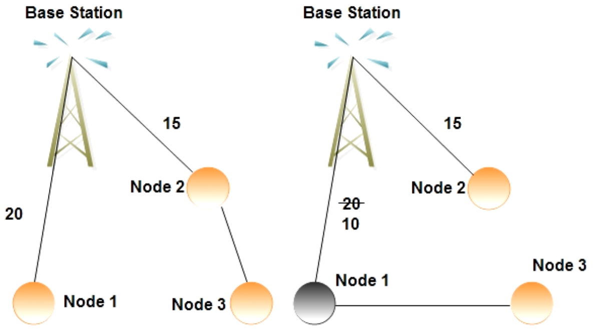


Figure 2 (a) WSN scenario without sinkhole node (b) WSN scenario with sinkhole node

To detect the sinkhole attacks in WSNs is a challenging task due to the dynamic nature and communication patterns of network. The sensor nodes communicate with base station and make a route through other nodes, and this is an open opportunity for intruders, where they capture and compromise the sensor node by modifying its contents. Various different types of approaches have been designed to addressed the sinkhole attacks based on detection, rule, prevention, hybrid and statistical approaches [13]. However, due to resource constraint nature of WSN, most of previous approaches are not suitable. In addition, the detection based approaches search anything unusual or can detect the node misbehavior in network [14]. On the other hand, rule based approaches are designed for intrusion detection systems, where every node sends and receive rules packet and monitor those nodes, which are violate the rules [15]. The statistical approaches are based on certain nodes activities. The prevention based approaches are refer to the node, where data authenticity and integrity of packets transmitted between the nodes with in the network. Finally, the hybrid approaches are composed with the combination of cryptographic and node abnormal behaviour detection to encounter sinkhole attacks [16]. The comparison of previous approaches are show in Table 1

Table 1 Proposed approaches for sinkhole attacks in WSN

S/No	Approach	Description
1	Centralized detection Approach [17]	In this work authors were proposed a centralized strategy to detect suspicious region in the WSN and using geo-statistical hazard model and distributed monitoring approach to overcome sinkhole attacks.
2	Agent detection based Approach [18]	The authors proposed an agent based approach to verify trusted node neighbors in three-step negotiation process which defend against malicious node.
3	Prevention Based Approach [19]	In this work authors proposed cryptographic approach based protocols RESIST-O and RESIST-1 to deal with sinkhole attacks.
4	Non Cryptography detection based approach [20]	In this work authors deployed mobile agent based defense mechanism using non-cryptographic approach against sinkhole issues in wireless sensor networks.
5	Prevention based approach [21]	The authors proposed cryptography based message digest protocol for sinkhole attack detection.
6	Hybrid Approach [16]	Author combined two approaches: signature and anomaly, which are based on detection mechanism of sinkhole and sleep deprivation attacks.
7	Detection based approach [14]	The authors proposed received signal strength indicator (RSSI) with the help of extra sensor node to perform monitoring and to detect sinkhole attack.
8	Detection and rule based approach [22]	In this work authors used rule-based approach to identify sinkhole attack.
9	Distributed rule and detection based approach [23]	Authors defined distributed rule-based detection mechanism to identify and exclude the sinkhole based compromised node from the network.

4.0 BLACKHOLE ATTACK IN WSN

Another severe security threat in WSN is a Blackhole attack, where intruder capture and compromised with a group of sensor nodes and creates a forged routing. This process blocks the data packets and turn the packets to the base station and encountered misbehavior attack. Due to this attack, the network disturbs and degrades the network performance in terms of increasing throughput and end-to-end delay. The Figure 3a, shows the total 9 nodes in network, where 6 (N1-6) nodes are normal and 2 (R1, R2) are routers and 1 coordinator node. The sensor nodes are sensing the data and further forward to coordinator node for further processing. Figure 3b depicts the Blackhole attack on router node (R2) in a network.

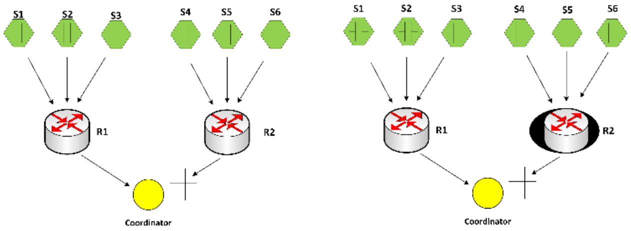


Figure. 3 (a) Normal data forwarding (b) Blackhole attack

In Figure 3 node R1 wants to send the data packets to R2 through coordinator node but R2 is compromised due to Blackhole attack and establish fake route by changing the routing table entries. Blackhole node absorbs all traffic from R2 and coordinator node and not forward the data packets to other nodes (SN4, SN5, SN6) for further processing. Due to Blackhole attack on R2, the data will not reach to destination node. The effect of Blackhole attack is observed in terms of decreasing throughput and gradually down the network performance.

Different strategies have been designed to address Blackhole issues in network. In the work [24] authors studied the security needs of Wireless Sensor Network (WSN), and briefly highlight the security properties. In another study [25] authors proposed novel approach about the detection of DoS attacks in cluster based network. Authors claimed the approach for decreasing energy consumption and improved network security. Some proposed studies related to Blackhole attack are presented in Table 2.

5.0 SIMULATION RESULTS

5.1 Blackhole Attack

The experimental evaluation is carried out through NS2 simulator where we evaluate the impact of Blackhole attack in Wireless Sensor Network (WSN). The simulation parameters are set with 8 sensor nodes, where 6 (n1-n6) are normal and 2 (r1, r2) are router nodes. The simulation running time is set with 60 minutes and coverage area is set with 200 X 200 meter.

Table 2 Proposed approaches for Blackhole attacks in WSN

S/No	Approach	Description
1	Deployment based approach [26]	In this study authors proposed a multiple base stations approach which is deployed in WSN to counter the impact of Blackhole on data transmission.
2	Detection based approach [27]	In this work authors proposed two modifications to lightweight medium access control protocol to deal with communication jamming and Blackhole issues.
3	Prevention based approach [28]	In this work authors studied and propose a protocol to deal with security in sensor network and to prevent against Denial of Service attacks.
4	Detection based approach [29]	In this study authors used intelligent agents called Honeypots which detects Blackhole attacks in wireless sensor networks.

In this first scenario we test the network under normal network conditions, without any compromised node, where sensor nodes are communicating with each other and with routers without any delay and packet dropping.

Results clearly show in Figure 5 the smooth network data flow with 0% drop ratio in the absence of Blackhole attack. In Blackhole attack malicious node falsely advertises wrong path information and with malicious intention to drop all data packets received as shown in Figure 6.

In Figure 7 clearly shows the results with Blackhole attack, where node compromised disseminate with high sequence number as a fresh route to the destination and packet dropping is on high level.

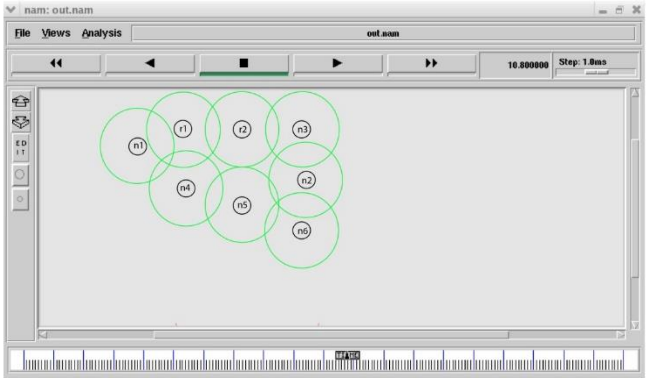
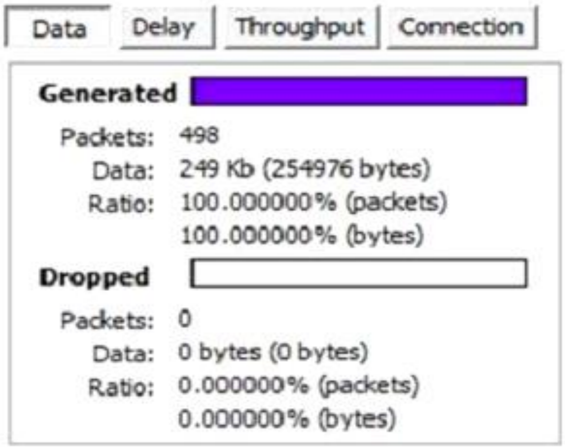


Figure 4 Sensor traffic flow without Black hole attack



Generated

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Dropped

Packets: 0
Data: 0 bytes (0 bytes)
Ratio: 0.000000% (packets)
0.000000% (bytes)

Figure 5 Network results without Blackhole attack

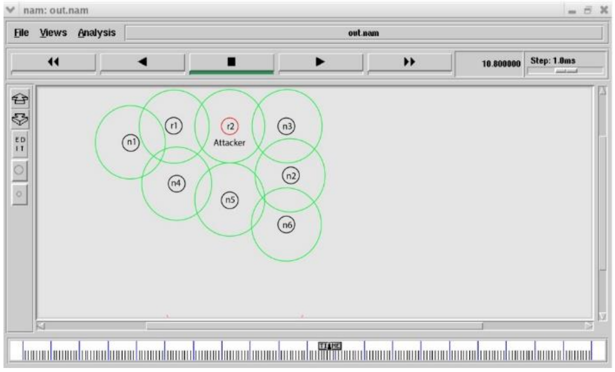
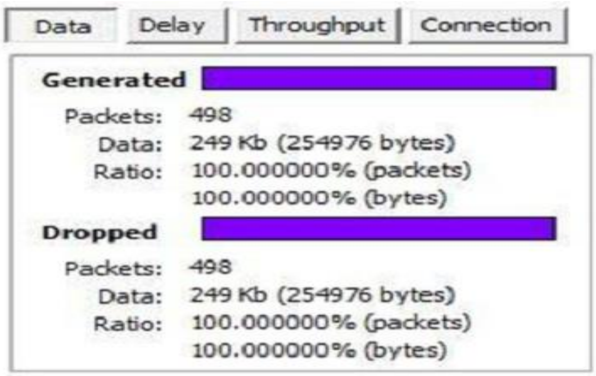


Figure 6 Blackhole attack in WSN



Generated

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Dropped

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Figure 7 Packet dropping in WSN

5.2 Sinkhole Attack

In order to check the effect of sinkhole attack in Wireless Sensor Network, by simulating in NS2 simulator. We formed the network with the parameters given table 4, in this first testing scenario network is configured normally without any Sinkhole attack. In simulation setup, the total sensor nodes are 4, where 3 are normal and 1 is base station. Simulation time is set with 15 minutes, with tree topology. The total coverage area is 200 X 200 meter. It is observed in Figure 8, that all 3 nodes (n1, n2, n3) are communicating normally with base station (s1), where node n3 sends the data packets by n2 and n1 respectively and send directly to base station.

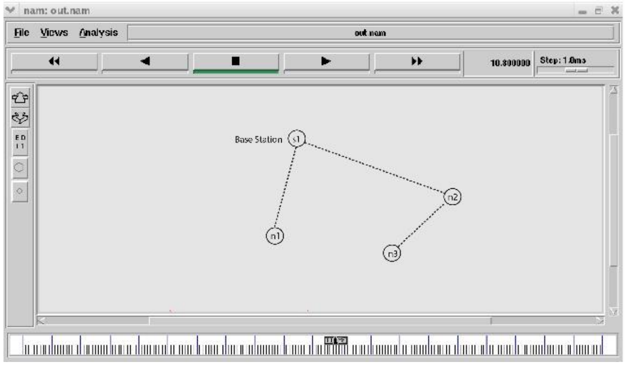
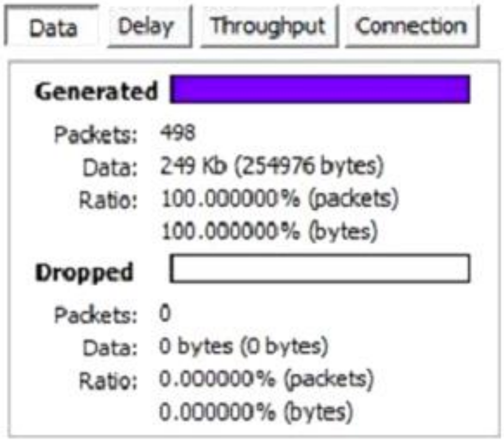


Figure 8 Normal process in WSN

Figure 9 clearly shows the normal flow of traffic in WSN and drop ratio is 0 %.



Generated

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Dropped

Packets: 0
Data: 0 bytes (0 bytes)
Ratio: 0.000000% (packets)
0.000000% (bytes)

Figure 9 Normal scenario with packet dropping

In second simulation setup, the operation of WSN with sinkhole attack is, Figure 10 clearly shows the effect of sinkhole and attract network traffic. Sinkhole attack disrupts the communication flow and offer quickest path to base station in a network. The sinkhole node comes with fake route information to base station. In this scenario node 3 is a malicious sinkhole node which drops all the packets and not forward any data to base station. Figure 11 shows the packet dropping due to sinkhole attack in network.

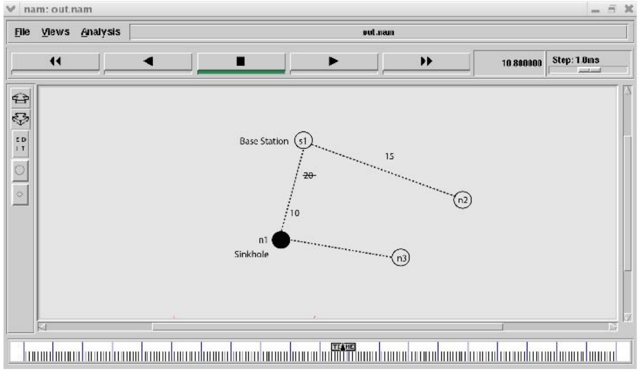
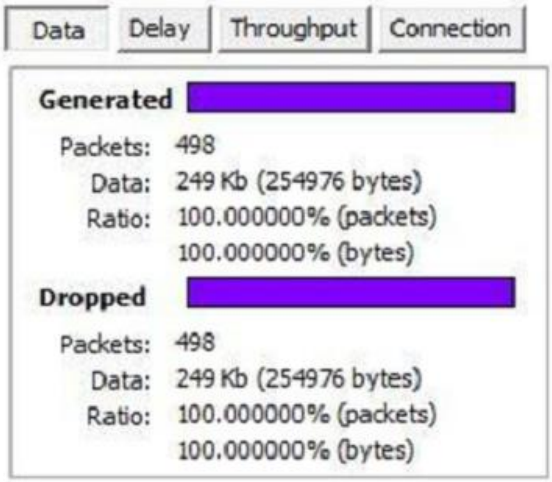


Figure 10 Sinkhole attack in WSN Network



Generated

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Dropped

Packets: 498
Data: 249 Kb (254976 bytes)
Ratio: 100.000000% (packets)
100.000000% (bytes)

Figure 11 Sink hole attack and Packet drop statistics

WSNs are constantly getting the attention due to the fact that they are used in various applications and domains. However, due to changing nature of these networks, different types of attacks make network vulnerable. Sinkhole and Black hole attacks are just a few examples of false communication and packet drop due to compromised nodes. In order to develop a secure system for these networks, design an efficient mechanism is still a challenge for scientific community. In order to protect network from these attacks different types of approaches have been proposed, but the limited energy and low battery power are main obstacles for the deployment of advance techniques.

6.0 CONCLUSION

Despite the widespread usage of Wireless Sensor Network (WSN), the network has been suffered from various attacks such as black and sink hole attacks. In these attacks, the network faces the end-to-end delay, packet loss issues. In this study, through simulation, we examined these two attacks and observed the network performance. Furthermore, the results showed that Therefore, there is a need to develop an secure and smart detection approach to prevent the network from any loss in terms of data packets and detect black and sink hole attacks earlier in network. After aforementioned review and experiment results, study recommended that the system architect should care about important security requirements in all levels. For future work, we plan to design and develop more complex sinkhole and black hole attack scenarios and explore more for future researchers.

References

[1] Rong, C.-m., Eggen, S., and H.-b. Cheng. 2011 .A Novel Intrusion Detection Algorithm For Wireless Sensor Networks, in Wireless Communication. *Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference*. 28 Feb- 3 March 2011. 1-7.

[2] Qureshi, K. N., and Abdullah, A. H. 2014 .Adaptation of Wireless Sensor Network in Industries and Their Architecture, Standards and Applications,. *World Applied Sciences Journal*. 30(10): 1218-1223.

[3] Qureshi, K. N., and Abdullah, A. H. 2013 .A survey on intelligent transportation systems. *Middle-East Journal of Scientific Research*. 15: 629-642.

[4] Qureshi, K. N., Abdullah, A. H., and Anwar, R. W. 2014. Wireless Sensor Based Hybrid Architecture for Vehicular Ad hoc Networks, *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 12(4): 942-949.

[5] Anwar, R. W., Bakhtiari, M., Zainal, A., and Qureshi, K. N. 2015 .A Survey of Wireless Sensor Network Security and Routing Techniques. *Research Journal of Applied Sciences, Engineering and Technology*. 9(11): 1016-1026.

[6] Chan, H., Perrig, A., and Song, D. 2003. Random Key Predistribution Schemes For Sensor Networks. *Security and Privacy. Proceedings. 2003 Symposium*. 97-213.

[7] Hwang, J., and Kim, Y. 2004. Revisiting Random Key Pre-Distribution Schemes For Wireless Sensor Networks. *Proceedings of the 2nd ACM workshop on Security Of Ad Hoc And Sensor Networks*. 43-52.

[8] Carman, D. W., Kruus, P. S. and Matt, B. J. 2000. Constraints And Approaches For Distributed Sensor Network Security (final). *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*. 1(1).

[9] Perrig, A., Szewczyk, R., Tygar, J., Wen, V., and Culler, D. E. 2002. SPINS: Security Protocols For Sensor Networks. *Wireless networks*. 8(5): 521-534.

[10] Eschenauer, L. and Gligor, V. D. 2002. A Key-Management Scheme For Distributed Sensor Networks. *Proceedings of the 9th ACM conference on Computer and Communications Security*. 41-47.

[11] Samundiswary, P., Sathian, D., and Dananjayan, P. 2010. Secured Greedy Perimeter Stateless Routing For Wireless Sensor Networks. *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*. 1(2): 9-20.

[12] Sen, J. 2009. A Survey on Wireless Sensor Network Security. *International Journal of Communication Networks and Information Security (IJCNIS)*. 1(2): 55-78

[13] Onat, I. and Miri, A. 2005. An Intrusion Detection System For Wireless Sensor Networks. *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*. 253-259.

[14] Tumrongwittayapak, C., and Varakulsiripunth, R. 2009. Detecting Sinkhole Attacks In Wireless Sensor Networks. *ICCAS-SICE*. Fukuoka, Japan. 18-21 August 2009 1966-1971.

[15] Tumrongwittayapak, C., and Varakulsiripunth, R. 2009. Detecting Sinkhole Attack And Selective Forwarding Attack In Wireless Sensor Networks, *in Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference*. 1-5.

[16] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G. 2010. An Intrusion Detection System For Critical Information Infrastructures Using Wireless Sensor Network Technologies. *Critical Infrastructure (CRIS), 2010 5th International Conference*. 1-8.

[17] Shafiei, H., Khonsari, A., Derakhshi, H., and Mousavi, P. 2014. Detection And Mitigation Of Sinkhole Attacks In Wireless Sensor Networks. *Journal of Computer and System Sciences*. 80(33): 644-653.

[18] Hamedheidari, S., and Rafeh, R. 2013. A Novel Agent-Based Approach To Detect Sinkhole Attacks In Wireless Sensor Networks. *Computers & Security*. 37:1-14.

[19] Le Fessant, F., Papadimitriou, A., Viana, A. C., Sengul, C., and Palomar, E. 2012. A Sinkhole Resilient Protocol For Wireless Sensor Networks: Performance And Security Analysis. *Computer Communications*. 35(2): 234-248.

[20] Sheela, D., Naveen, K., and Mahadevan, G. 2011. A Non-Cryptographic Method Of Sink Hole Attack Detection In Wireless Sensor Networks. *Recent Trends in Information Technology (ICRTIT), 2011 International Conference. Chennai, Tamil Nadu*. 3-5 June 2011. 527-532.

[21] Sharmila, S., and Umamaheswari, G. 2011. Detection Of Sinkhole Attack In Wireless Sensor Networks Using Message Digest Algorithms,. *in Process Automation, Control and Computing (PACC), 2011 International Conference*. Coimbatore, Tamil Nadu. 20-22 July 2011. 1-6.

[22] I. Krontiris, T. Giannetsos, and T. Dimitriou. 2008 .Launching A Sinkhole Attack In Wireless Sensor Networks; The Intruder Side,. in Networking and Communications, 2008. WIMOB'08. *IEEE International Conference on Wireless and Mobile Computing*. 526-531.

[23] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, 2008 .Intrusion Detection Of Sinkhole Attacks In Wireless Sensor Networks,. in Algorithmic Aspects of Wireless Sensor Networks, ed: Springer. 150-161.

[24] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, 2008 .Security In Wireless Sensor Networks,. *Wireless Communications And Mobile Computing*. 8: 1-24.

[25] M. Guechari, L. Mokdad, and S. Tan. 2012 .Dynamic Solution For Detecting Denial Of Service Attacks In Wireless

Sensor Networks,. *in Communications (ICC), 2012 IEEE International Conference on*. 173-177.

[26] S. Misra, K. Bhattarai, and G. Xue. 2011 .BAMBi: Blackhole Attacks Mitigation With Multiple Base Stations In Wireless Sensor Networks,. *in Communications (ICC), 2011 IEEE International Conference on*. 1-5.

[27] A. R. Mahmood, H. H. Aly, and M. N. El-Derini. 2011 .Defending Against Energy Efficient Link Layer Jamming Denial Of Service Attack In Wireless Sensor Networks,. *in Computer Systems and Applications (AICCSA), 2011 9th IEEE/ACS International Conference on*. 38-45.

[28] R. Nanda and P. Venkata Krishna. 2011.A Self Enforcing And Flexible Security Protocol For Preventing Denial Of Service Attacks In Wireless Sensor Networks,. in Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE. 847-850.

[29] A. Prathapani, L. Santhanam, and D. P. Agrawal, 2009 .Intelligent Honeypot Agent For Blackhole Attack Detection In Wireless Mesh Networks,. in Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on. 753-758.