International Journal of Electrical, Electronics and Computer Engineering **5**(1): 33-40(2016)

ISSN No. (Online): 2277-2626

Optimized AODV Routing for Effective Attack Security in Wireless Sensor Networks

Anand Motwani* and Vimal Dhote**

**Assistant Professor & Head, Department of Computer Science & Engineering, NRI Institute of Research & Technology, Bhopal, (Madhya Pradesh), INDIA*

***M. Tech. Scholar, Department of Computer Science & Engineering, NRI Institute of Research & Technology, Bhopal, (Madhya Pradesh), INDIA*

(Corresponding author: *Vimal Dhote)*

(Received 10 March, 2016 Accepted 07 April, 2016)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless Sensor Networking is one of the most hopeful technologies that have wide range of applications ranging from home surveillance, military to Internet of Things (IoT). Although Wireless Sensor Networks (WSNs) have attractive features like: less deployment cost and least attended network operation, the security of such networks is a big concern especially when such networks are deployed for critical applications. Therefore, in order to securely operate the WSNs, any kind of intrusions should be determined before attackers can affect the network. In a type of WSNs, multiple nodes would send sensor readings to a base station (Sink) for further processing. Such a many-to-one communication is highly vulnerable to a sinkhole attack. In this attack an attacker replies with false routing information, to the nodes that want to communicate (send information to sink). This attack is a serious threat to WSNs, because the nodes are generally deployed in open areas and have weak computation and battery power. In this paper a survey of the state-of-the-art in 'attacks and counter measures' (Intrusion Detection Systems) that are proposed for WSNs are presented. Finally, this work suggests the Optimized AODV Routing with "Alert based" technique to enhance the security of WSNs from sinkhole like attacks. The same is achieved by implementing four processes: Setup process, Identifying attacker, Eliminating it, and Optimizing the route. It is promising that, this technique is improving the QoS parameters like Delay and Packet Delivery Fraction in WSNs, while detecting and eliminating the malicious node efficiently. The work quantitatively analyze some of the desirable properties of WSNs routing protocols to craft a more secure and reliable WSNs. For simulation purpose, famous Network Simulator version (ns – 2.33) is used.

Keywords: Mobile Ad-hoc Network (MANET), Wireless Sensor Network (WSN) Routing Security, Attacks, Intrusion Detection System (IDS), Sinkhole attack, Black hole attack, Attack Detection, Attack Prevention, AODV, Quality of Service (QoS), Network Simulator (NS-2).

I. INTRODUCTION

Typically, a spatially distributed network of tiny wireless mobile devices for sensing and sending event information, called sensor nodes, can be defined as Wireless Sensor Network (WSN). The data collected by different nodes is sent to a node known as Sink which either uses the data locally or is connected to other networks. Fig. 1 depicts a typical WSN where sensor nodes are deployed in ad-hoc manner.

These nodes are mobile and capable of sensing the events. These nodes are equipped with a wireless radio, generally based on IEEE 802.15.4 radio to communicate among them. The nodes have short radio-range (less than 100 m) and low-rate (10 – 250 kbps). The power source is rechargeable batteries with limited capacities. Since the radio consumes maximum battery power it must incorporate energy-efficient communication techniques.

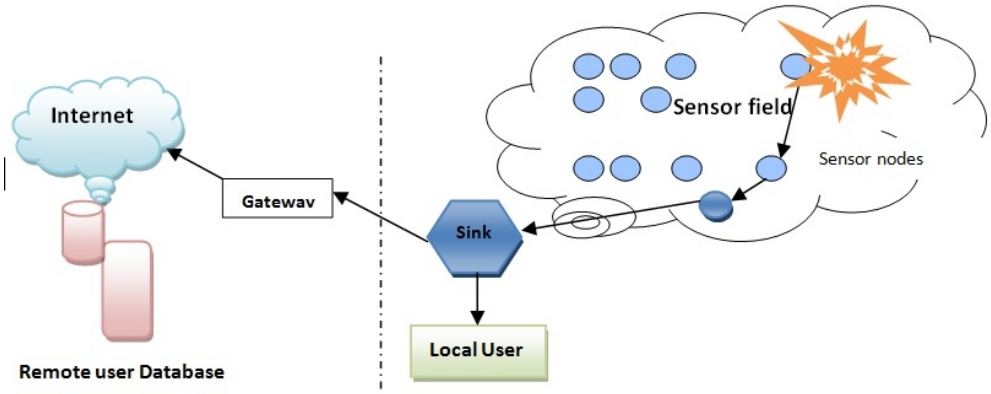

Fig. 1. A Typical WSN.

Wireless Sensor Network (WSN) is one of the most promising and emerging technologies for the future. WSNs are easily deployable, small, inexpensive, and cost effective. However, WSN market is forecast to grow up to $2 billion in 2022 [1], a variety of challenges that facilitate the widespread use of WSN technology in real-world domains need to be addressed. The challenges also include security. Protocols of data transmission in WSNs are simpler and more vulnerable to a variety of attacks than protocols designed for wireless mobile or ad hoc networks [2]. Mobile WSN consists of mobile sensor nodes that can move around and interact with the physical environment. In addition to be able to sense, compute, and communicate the mobile sensor nodes can reposition and organize themselves in the network. A dynamic routing algorithm must be employed in WSN. In literature, many routing protocols for sensor network have been proposed; few of them have been designed with security as a goal. Various security issues and threats that are considered for wireless MANET can be applied for WSN [4]. WSN are simple so susceptible to routing attacks [3]. Among five types of WSN presented in [8], we only address Mobile WSN which is relevant to our work.

The researchers are focusing on using improved versions of existing routing protocols over IEEE 802.15.4 based sensor networks and also developing new routing protocols. One such work is done and presented in [12], where improved AODV routing protocol is proposed and analyzed for performance in sensor networks. The special properties of WSN constrain many misbehavior types; but AODV is vulnerable to various kinds of attacks, as described in [11].

AODV mechanism is simple and it has no security features [6, 9]. Nodes with malicious intent can easily setup various kinds of attacks [10]. Here, availability and integrity attacks [11] are considered in which packets are dropped (complete or partial).

This work typically involves attack defense (detection and prevention) of sinkhole attacks by providing Optimized AODV routing. Optimized routing also increases the efficiency and reliability of routing protocol in terms of QoS. To introduce some security improvements in routing protocol (AODV) that deal network layer attack and provide optimized route for communication is the objective of this research in WSN.

II. RELATED WORK (ATTACKS AND COUNTER MEASURES IN SENSOR NETWORK ROUTING)

Various security issues and threats that are considered for wireless ad hoc network can be applied for WSN [4]. The WSNs are susceptible to routing attacks by malicious nodes and packets are dropped in attacks like sink-hole attack. The limited power and memory of sensor nodes makes conventional security solutions impractical. Among a range of intrusion detection algorithms available, the selection of the Technique for intrusion detection would be specific to the application's requirements i.e., the attacks that need to be detected and the accuracy of the detection. For example for stationary applications, centralized IDS schemes are preferred in literature as they are powerful enough to detect whole range of attacks. To address another issue like amount of energy consumption, hierarchical model for IDSs is preferred.

The IDS should spend the least amount of energy as possible because energy is crucial matter for operations of the WSN. The literature [4, 16] presented a survey of the state-of-the-art in IDSs and efforts made to overcome them. The impact of malicious attacks on the performance of a sensor network is studied in various works including [5, 24, 26].

The attack detection schemes belong to two major classes': Computationally Limited and Computationally Intensive. The schemes proposed in [7, 17, 18, 19, 20] belong to first and [21, 22, 23] belong to second class of attacks.

The authors [16] presented a survey of the state-of-the-art in IDSs (Intrusion Detection Systems) proposed for WSNs. They stated that IDSs are functionally categorized into three groups: anomaly based detection, misuse based detection, and specification based detection: The IDSs proposed for Mobile Ad-Hoc Networks (MANETs) and applicability of those systems to WSNs are discussed. IDSs proposed for WSNs and guidelines that are potentially applicable to them are also provided with their advantages and disadvantages. They concluded by highlighting open research challenges in the field.

In another work, the authors [3] propose security goals for routing in sensor networks. They demonstrated how attacks against ad-hoc networks can be adapted into powerful attacks against sensor networks. Two classes of novel attacks against sensor networks—sinkholes and HELLO floods are introduced, and analyze the security of the major routing protocols for sensor networks. They also suggested countermeasures and design considerations. The best solution suggested for wormhole and sinkhole detection is careful design of routing protocols which avoid routing race conditions and make these attacks less meaningful.

Edith C.H. Ngai *et al.* [13] stated that a many-to-one communication where multiple nodes send sensor readings to a sink node (base station), is highly vulnerable to a sinkhole attack. A sinkhole attack considered as a serious threat to sensor networks deployed in open areas with weak computation and less battery power. Authors proposed a new technique for detecting the attacker. The algorithm first prepares list of suspected nodes through checking data consistency, and then effectively identifies the intruder from the list by analyzing the network flow information. This algorithm is robust to deal co-operative attacks. Although it has the reasonable computation overheads, the proposal comes under computational intensive category.

In depth study of sinkhole attack launching in realistic networks with Mint Route routing protocol is done [25]. The appropriate rules in IDS system are embedded to enable its detection successfully. They demonstrated the work in their own sensor network deployment confirm the effectiveness and accuracy of the algorithm in the general case of random topologies.

III. PROPOSED: OPTIMIZED AODV ROUTING FOR EFFECTIVE ATTACK SECURITY IN WSN

This scheme proposes to setup a process at every node in network. This is less costly in terms of overhead and more appropriate to AODV because the process setup time is in between generation of RREQ and dissemination of control messages.

The proposed work involves four phases, which are described below:

A. Pre Configuration Phase (Initialization or Setup Phase)

In our implementation of proposed work, the process starts when routing protocol operation begins and remains active till the time a reliable communication is established between source and sink. In case node goes down or when node goes out of the transmission range or in case any route error occurs, the process setup begins again. Two typical cases for communication establishment are identified by study and addressed here:

Case I: If node neither communicated earlier i.e. it is communicating first time. And, when multiple replies received including reply from sinkhole node came. Simply it is the case when attacker replies from within the transmission range.

When a NODE wants to communicate with some unknown destination (sink), it prepares itself by setting up few parameters. In proposed work one of it is 'destination sequence number', which is set at a static threshold value. Threshold value of can be calculated dynamically by some previous transactions/communication with other nodes. Another purpose of setting up of the threshold value is to avoid the possibility of co-operative sinkhole attacks.

Another one is special capability of checking specific alert, in recvReply() function. The special alert is not expected to come from sinkhole. In this case the sender node has to take risk of sending through only node in its range. Only case where sender gets feeling of transmission but it may or may not happen. In this case setting up of special alert works

Case II: Another case where the only reply is received from sinkhole.

To deal with such case, the setting up of some Special alert in the receive reply function helps in trust establishment and ensures that the control message is from known network node. So in the next phase of Detection, the process established at node checks each reply arrived. The node can be source or intermediate node.

B. Identification (Detection) Phase

In this phase the detection of sink hole is carried out by testing the special alert defined above. The capability of checking specific alert, which is not expected to come from sinkhole, in recvReply() function distinguish this work from others. The sink holes are identified at time route setup time, so less overhead is imposed by the proposed solution.

C. Prevention Phase

In this phase either the node is ignored (their participation is not counted) and not used for forwarding data packets anymore. To prevent its further participation the Routing table is not updated on such reply.

D. Route Optimization Phase

During the same process (i.e. while detection) the destination sequence number received by destination or intermediate node is compared with threshold value. If the value received is greater than this threshold then the control packets are dropped. Then value with highest destination sequence number, of-course which is less than threshold along with lesser hop-count is saved as optimal path. In this way the same routing path is saved and followed till route error or break. Thus, Optimal Routing takes less route setup time and will not overhead the network.

IV. EXPERIMENTAL SETUP AND RESULT ANALYSIS

A. Simulation Setup

The simulations were conducted on a PC with an Intel Pentium Dual Core processor at 2.5GHz. , 4 Giga Bytes of RAM, running Red Hat Enterprise Linux 5.0 as Operating System. Network Simulator version 2.33 (ns-allinone-2.33) [27] is used for simulation purpose.

The studied scenario consists of network of wireless nodes having 25 mobile sensor nodes randomly distributed over a rectangular area with 1000m x 1500m. The sinkholes' are also kept mobile like other mobile sensor nodes to create nearly real scenario. Two scenarios are considered for simulation. In first, one sensor node out of 25 mobile sensor nodes is generating constant bit rate (cbr) traffic and sending packets to Sink (receiver). In second scenario, two sources are sending packets to sink. Farthest nodes are chosen as sources so that they should be enough hop distance away from Sink (destination). The sending time of data packets from 2 traffic sources is chosen randomly within the time of the simulation.

All the parameters that are general to all the simulations conducted in this work are summarized in Table 1.

Table 1: General Simulation Parameters.

Parameter	Value
Transmission range	100 m
Wireless Bandwidth	250 Kbits/sec
Simulation time	300s
Number of mobile nodes	25
Number of sources	01 (scen-1), 02 (scen-2)
Number of receivers	01
Number of connections	02
Number of Scenario	02
Number of sinkholes	02
Traffic type	Constant bit rate (cbr)
Packet rate	5 Packets/sec.
Packet size	512 bytes
Pause time	10.0 sec.
Minimum speed	1m/sec.
Maximum speed	20m/sec.
Routing protocol	AODV
MAC protocol	802.15.4

To see the effect of presence of sinkhole in WSNs and how the proposed scheme performs better than AODV, and AODV with attack in WSN, AODV once simulated without attacks and then with attack and then with proposed solution.

B. Result Analysis and Discussion

The researchers are interested to measure the metrics, when studying routing protocols in MANETs, are used to evaluate the performance of WSN.

The performance metrics of WSN is first evaluated for 'WSN with normal AODV [15] protocol', 'WSN with sinkhole attack affected AODV' and 'WSN with proposed Optimized WSN' in two Scenarios (cases): The scenario – 1 and 2 respectively consists of one & two traffic sources. The metrics along with results are shown below:

Packet Delivery Fraction (PDF): The packet delivery ratio is defined as the number of received data packets at the destinations divided by the number of generated data packets by the sources. The graph shown in Figure 2 compares the PDF for all cases. The result shows that such attacks are more hazardous when more senders involve, which is most common case in WSNs. On applying proposed "Optimized Routing with Attack Defense" the performance of AODV even under attacks is increased twice in case of 2 senders. This shows that the proposed scheme in WSNs will improve the network performance and reliability.

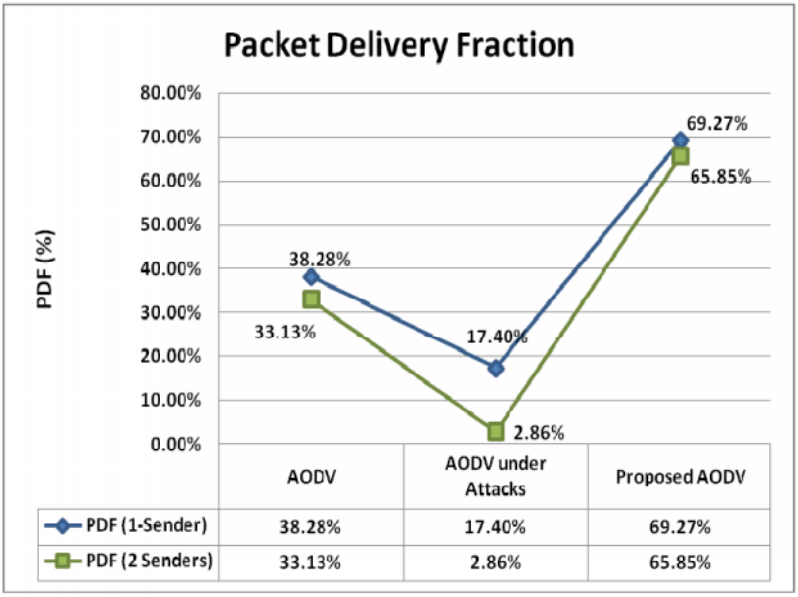

Fig. 2. Comparison of Packet Delivery Fraction.

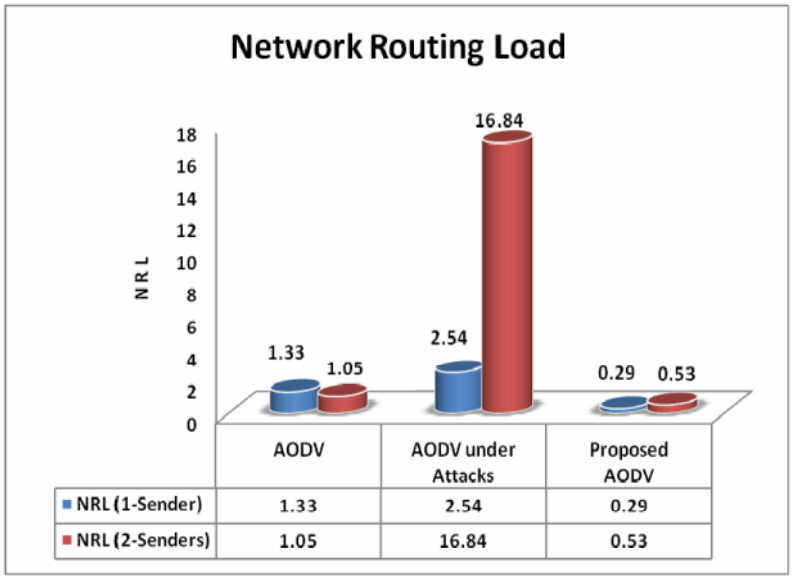

Fig. 3. Comparison of Network Routing Load.

Network Routing Load (NRL) [14]: It is the percentage of total routing packets and total data packet ratio transmitted in the network. The result shows that NRL is tremendously increased as a result of attack. The proposed scheme not only decreases network routing load but also provides optimal path for communication while removing the attacks. Figure 3 shows NRL in all cases. Optimal path found by proposed modification is better in terms of routing load in WSNs.

End-to-End Delay: This is defined as the time required for a packet to travel from source to destination.

As the time for each packet is variable, average end to end delay is calculated. Figure 4 shows the average end to end delay comparison of all discussed versions (including proposed) of the protocols. Optimal path found by proposed modification in AODV protocol is better in terms of delay also.

Number of Packet Dropped: Total number of MANET packets dropped out of total number of generated packets. Figure 5 show the comparison between numbers of packets dropped using the protocols in two different scenarios discussed earlier.

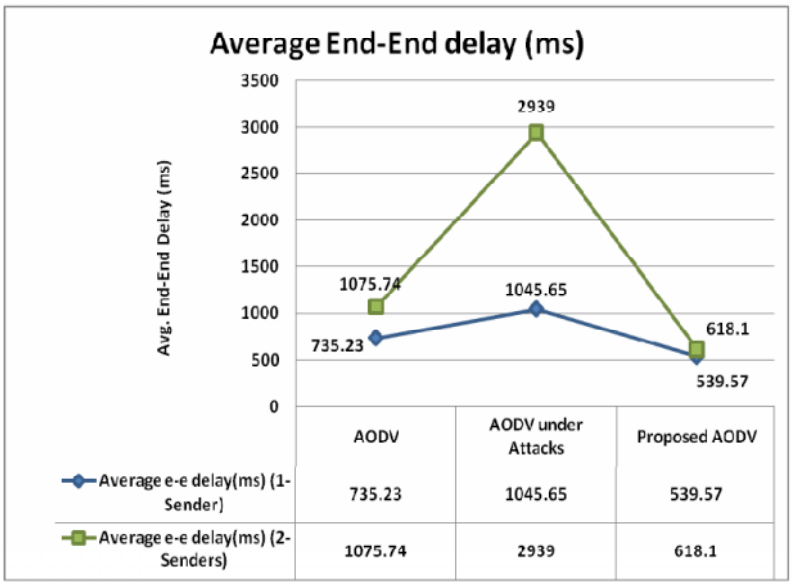

Fig. 4. Comparison of Average End to End Delay.

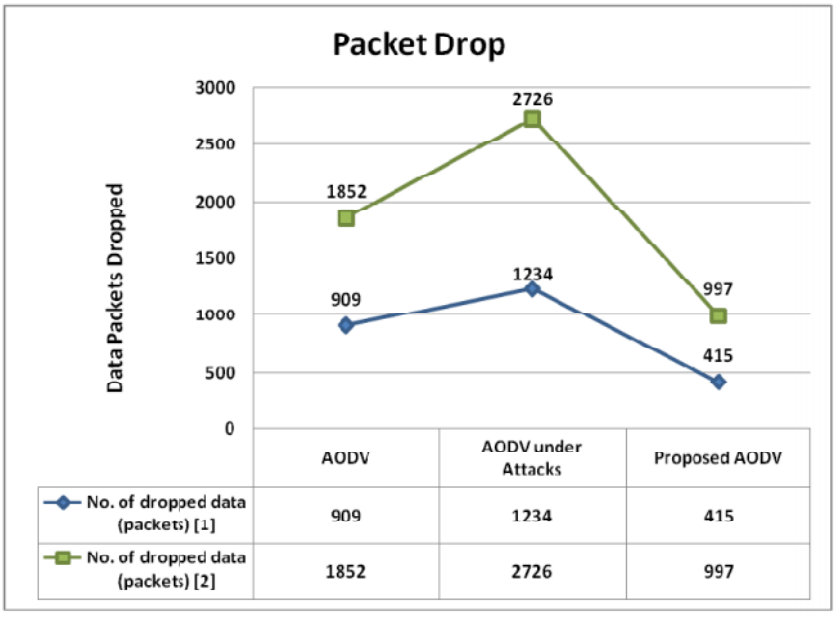

Fig. 5. Comparison of Number of Packets Dropped.

V. CONCLUSION AND FUTURE WORK

A. Conclusion

In this work, an attempt is made to show the effect of sinkhole attack which is a dreaded network layer attack and formalize the problem of intrusion defence in WSNs. Another issue which is addressed is finding optimal route for better quality route and reliable communication in WSNs. The necessary and sufficient conditions for successfully revealing the attacker and optimal routing are presented in general WSN model. The Proposed "Optimized AODV Routing for Effective Attack Security in WSNs" defends sinkhole attacks and improves WSN performance. "Alert Based" technique and Route Optimization is respectively used for defending attack and improving routing.

Through simulation results we compared AODV, AODV under attacks and proposed Optimized AODV. Numbers of Packet delivered are fewer in case of AODV and AODV under sinkhole attack. On increasing just one sender the PDR is dropped by 97% in AODV with sinkhole attack. We can say sinkholes are more vulnerable in case of increased senders. The network is near to failure in case of 2 senders and two sinkhole attackers. Also, the End-to-End Delay, NRL and Packet Drops are more in AODV and AODV under sinkhole attack, while it is maintained at good level in proposed AODV. The quality of proposed work can be judged by its reliability in terms of PDR and its quality by End-to-End Delay and NRL. The proposed work outperformed in terms of reliability and quality.The results demonstrated that solution is reliable and effective in terms of quality parameters. The communication and computation overheads are reasonably less as the proposed method is implemented in existing functionality.

B. Future Work

The implementation demonstrates that the AODV can be efficiently used to run on sensor nodes. Thus, studying the application of more such dynamic routing protocols in wireless sensor networks is a viable research direction. Although individual proposal to specific attacks might be more efficient, further investigation of proposal can provide even more attractive solutions for defending such types of networks against intrusion. In future, the proposed work can be further tested on variety of different scenarios and with energy aware routing protocols for WSNs.

REFERENCES

[1]. Harrop P (2012). Wireless sensor networks and the new Internet of things. Energy Harvest J. Available at http://www.energyharvestingjournal.com.

[2]. C. Karlof, D. Wagner, (2003). "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, 2003.

[3]. Chris Karlof, David Wagner, (2003). "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks 1 (2003) 293–315, 2003 Elsevier B.V.

[4]. Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, (2010). "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network", *International Journal of Network Security & Its Applications (IJNSA)*, Vol. **2**, No.3, July 2010.

[5]. Neha Shrivastava and Anand Motwani. (2013). Article: Survey of Malicious Attacks in MANET. *International Journal of Computer Applications*, **80**(14):28-30, October 2013.

[6]. Vimal Dhote, Anand Motwani and Jyoti Sondhi. (2015). Article: A Review on Black Hole Attack in Mobile Adhoc Network. *International Journal of Computer Applications*, **116**(11):1-5, April 2015.

[7]. Roopal Lakhwani, Sakshi Suhane and Anand Motwani. (2015). Article: Agent based AODV Protocol to Detect and Remove Black Hole Attacks. *International Journal of Computer Applications* **59**(8):36-39, December 2012.

[8]. Yick J, Mukherjee B, Ghosal D, "Wireless sensor network survey". (2008). *Comput Netw*, **52**(12): 2292– 2330.

[9]. Htoo Maung Nyo, Piboonlit Viriyaphol "Detecting and Eliminating Black Hole in AODV Routing" 978-1-4244-6252-0/11/2011 IEEE.

[10]. Y. C. Hu, A. Perrig, and D. B. Johnson, (2005). "Ariadne: a secure on-demand routing protocol for ad hoc networks," in Wireless Networks (WINET), *ACM and Springer*, **11**(1-2): 21-38, January 2005.

[11]. Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs" 978-1-61284-307-0/11/2011 IEEE.

[12]. Yu-Doo Kim, Il-Young Moon, Sung-Joon Cho, (2009). "A Comparison Of Improved Aodv Routing Protocol Based On Ieee 802.11 And IEEE 802.15.4", *Journal of Engineering Science and Technology*, Vol. **4**, No. 2 (2009) 132 – 141.

[13]. Edith C.H. Ngai , Jiangchuan Liu, Michael R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", *ELSEVIER, ScienceDirect, Computer Communications*, **30** (2007) 2353–2364.

[14]. Johnson DB, Maltz DA (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. In: *Imielinski T, Korth H (eds) Mobile Computing*, vol. **353**. Kluwer Academic Publishers, pp 153–181.

[15]. C. Perkins, E. Belding-Royer, S. Das. (2003). "Ad hoc On-Demand Distance Vector (AODV) Routing" Feb. 2003 http://www.ietf.org/internet-drafts/draftietf- manet-aodv-13.txt.

[16]. Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, (2014). "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", *IEEE Communications Surveys & Tutorials*, VOL. **16**, NO. 1, FIRST QUARTER 2014.

[17]. H. Khattak, Nizamuddin, F. Khurshid and N. u. Amin, "Preventing black and gray hole attacks in AODV using optimal path routing and hash," Networking, Sensing and Control (ICNSC), *2013 10th IEEE International Conference* on, Evry, 2013, pp. 645-648.

[18]. P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 902-906.

[19]. Al-Shurman, M. Yoo, S. Park, (2004). "Black hole attack in Mobile Ad Hoc Networks", in Proc. ACM Southeast Regional Conference, pp. 96-97, 2004.

[20]. Kamarularifin Abd Jalil & Zaid Ahmad, Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing *Protocol" 2011 IEEE Conference on Open Systems (ICOS2011)*, September 25 - 28, 2011, Langkawi, Malaysia.

[21]. S. Gambhir and S. Sharma, "PPN: Prime product number based malicious node detection scheme for MANETs," Advance Computing Conference (IACC), 2013 *IEEE 3rd International, Ghaziabad*, 2013, pp. 335-340.

[22]. Payal N. Raj and Prashant B. Swadas, (2009). "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET", *International Journal of Computer Science Issues (IJCSI)*, Vol. **2**, Issue 3, pp: 54-59, 2009.

[23]. Nishu Kalia, Kundan Munjal (2013). "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol", *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume **2**, Issue 3, February 2013.

[24]. S. Rajanarayanan and C. Suresh Gnana Dhas, (2015). "Black Hole Attack Performance Evaluation and Degradation in Wireless Sensor Networks", *Middle-East Journal of Scientific Research*, ISSN 1990-9233, **23**(8): 1741-1748, 2015.

[25]. Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks".

[26]. S. Rajanarayanan and C. Suresh Gnana Dhas, (2015). "Black Hole Attack Performance Evaluation and Degradation in Wireless Sensor Networks", *Middle-East Journal of Scientific Research*, ISSN 1990-9233, **23** (8): 1741-1748, 2015.

[27]. Network Simulator-2, Available at: www.isi.edu/nsnam/ns.