Simulation of Wormhole Attack in Wireless Sensor Networks using AOMDV Protocol

J. Amutha
School of Information and Communication Technology
Gautam Buddha University,
Greater Noida
Uttar Pradesh, India

Rumaisa Azhar
School of Information and Communication Technology
Gautam Buddha University,
Greater Noida
Uttar Pradesh, India

Sandeep Sharma
School of Information and Communication Technology
Gautam Buddha University,
Greater Noida
Uttar Pradesh, India

ABSTRACT
Wormhole attack, a resource depletion attack being considered as one of the severe attack in Wireless Sensor Networks (WSN). It can interfere routing process at any time, drain the battery power of sensor nodes and also can disable the whole system. Hence, this work deals with a technique to identify and prevent wormhole attack using Adhoc On-demand Multipath Distance Vector (AOMDV) protocol. The main purpose of using AOMDV protocol is route discovery, multipath routing, network load handling, increases reliability and avoid the risks of congestion. The proposed technique is implemented in NS2.35 simulator and various performance parameters are evaluated.

Keywords
WSN, Wormhole attack, Round Trip Time, AOMDV

1. INTRODUCTION
Wireless Sensor Networks (WSN) are formed by a large collection of tiny sensor nodes that are responsible for sensing and monitoring the physical or environmental conditions [1]. Then the information is being transmitted to the WSN base station through single or multi-hop communications [2]. It also performs various other tasks such as computation, self-configuring the network and signal processing. Wireless sensor networks are used in various applications like monitoring weather and environmental conditions, health care, military etc.,[3]. Due to its dynamic nature, it is easy for the intruders to interfere the legitimate traffic. This leads to various issues concerning security like secrecy, privacy, key establishment, authentication, secure routing, etc., [4]. Authentication of nodes in wireless networks plays a vital role due to its openness [5]. The sensor nodes are also vulnerable to various kinds of attacks because of their restricted energy constraints like [6] limited battery life cycle, limited memory, low computation power and low bandwidth[7].

The different kinds of attacks in WSN include flooding, jamming, cloning, tampering, selective packet drop, denial-of-service, blackhole, wormhole, etc. One of the Denial of Service (DoS) attack is the flooding attack in which the attackers sends large amount of traffic through fake messages to collapse the entire service, causes congestion in the network and brings down the whole network [8]. Another DoS attack is the jamming attack in which the attacker interferes the radio signal. The attacker performs this intentionally to disturb the message communication between the sender and the receiver or to jam the area [9]. Clone attack is also known as node replication attack which can be deployed directly into the operations of the sensor networks and claims an identity similar to the operations performed by the legitimate node. It is considered as one of the most harmful attack and vulnerable in nature because it can access the security credentials, the keys and other parameters [10]. Tampering is also known as node capturing, which is the result of physical access like updation, alteration and destruction of the sensor node by the attacker [11]. Selective Packet drop is one of the active type of attacks and also considered as the partial denial of service attacks. This attack is performed in the sensor network by the malicious node which drops the packets instead of forwarding them to the destination node [12]. Denial of Service attack physically destroys the components of the sensor network. Each OSI layers of wireless sensor network has different types of Denial of Service attack [13]. In a black hole attack, the attacker node broadcast itself to the destination node falsely by using its routing protocol [14]. This attack always retains the data packet by the route request reply message which results in the depletion of the network performance [15]. Among these attacks, wormhole attack is considered the most hazardous attack in WSN [16].

Many solutions have been proposed to prevent the attacks such as routing protocols, [17] key exchange, authentication, etc. but they could not eradicate the attacks completely [18]. Therefore, security in WSNs face a great challenge against various types of attacks and is considered one of the most critical characteristics of any communication network [19].

1.1 Wormhole Attack in WSN
In wormhole attack, "tunnels" are formed by a pair of attackers, for transferring the routing messages between one sensor node location to another sensor node location and replays them locally in the network [20].

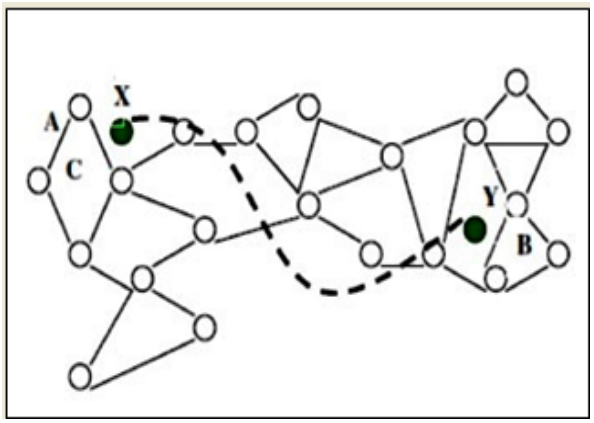

Fig 1: Wormhole Attack [22]

The tunnels are established by in-band or out-of-band channel. The wormhole attack by in-band channel is formed by building an overlay tunnel over the wireless medium. Out-of-band performs the attack by using various wireless network. Wormhole attack has a serious effect against routing protocols. The routing messages are tunneled by the attackers in wrong direction, thus making routing mechanisms get disrupted and confused [21]. This results in generating a fake route which acts as the shortest route than the established original route. The working principle behind wormhole attack is depicted in Figure 1. Node X receives the packet and is replayed through the node Y. Similarly the reverse process happens for node Y to node X. The attacker provides false information to node A and node B pretending as their neighbors to forward the routing messages. Then the routing messages are being selectively dropped and thus interrupt the communication between node A and B [22].

1.2 AOMDV Protocol

One of foremost aim of AOMDV protocol is multiple path discovery between the source senor node and the destination sensor node. Here, a routing table is maintained and a sender node checks the routing table for establishing the communication between two nodes by the route discovery process. If the route is present, then the routing table provides the routing information, otherwise it broadcast Route Request Packet (RREQP) to its neighbors. The neighbor node after receiving this packet checks the routing table for a route to the destination node [23]. When it is present, the source node sends the Route Request Packet and it receives the Route Reply Packet(RREPP) all along the same established path. The routing table contains the path information of every sensor nodes and thus the routes are established [24]. Based on the routing mechanism, AOMDV selects the main path among the multiple paths for transmission of routing messages. The other paths become effective only when the main path is unable to broadcast the messages.

2. RELATED WORK

The literature review is carried out on the basis of wormhole attack and AOMDV protocol. A resistant scheme for wormhole attack known as label-based secure localization was proposed by Chen et al. This scheme detect the wormhole attack and then defend against it by the DV(Distance Vector) Hop localization process. For each node, the scheme identify their pseudo-neighbors and secure localization is achieved by the communication link. The DV-Hop localization process contains three phases. A distance vector routing mechanism is achieved in the first phase, the second phase calculates the average distance of each hop and in the third phase estimates the distance. Then each sensor calculates its own location by other schemes like maximum likelihood estimation or triangulation method. Simulation results shows the effectiveness of this scheme for different parameters [25].

An efficient method for detecting and preventing the wormhole attack using AOMDV protocol was investigated by Amish et al. During route discovery process, the proposed protocol computes multiple paths for transmitting data. An algorithm is being designed and simulation is done using NS-2 Simulator based on the Round Trip Time mechanism[23].

Kumar et al. [26] developed a localization algorithm for mobile environment which is used to prevent wormhole attack. The algorithm incorporates Maximum Likehood Estimation (MLE) scheme to support the nodes mobility and thus results in adaptability of dynamic environments.

A routing protocol SeRWA for secure wireless sensor networks was proposed by Madria et al. [27] to prevent wormhole attacks in WSN. Using neighbor discovery and route discovery process, SeRWA protocol provides a secure route which acts against wormhole attack. The main aim of this protocol is that it does not require any hardware like GPS or synchronized clock to prevent the wormhole attack.

Bagade et al. proposed a wormhole attack detection system called Jitworm. It detects the wormhole attacks by fixing the threshold value with variable delays. A wormhole attack is suspected if the system contains no jitter. The variable delays are considered at the time of route establishment and transmission of data [28].

Various routing protocols in wireless sensor networks like OLSR, AODV, and ZRP with wormhole attacks was investigated by Govindasamy et al. A comparison is made for the different performance metrics such as energy consumption, delay, throughput in the static and dynamic WSN environment. The result shows that AODV has the overall better performance when compared with the other two routing protocols such as OLSR and ZRP. The future work focus on designing a protocol for secure routing to identify and prevent threats in wireless sensor networks [29].

Qazi et al. [20] proposed a M-Delphi (Multirate-Delphi) protocol to prevent wormhole attacks that adapts to 802.11 wireless channel. The main aim of the protocol is to provide neighbor monitoring, multirate channel and processing delay. This protocol is implemented in different simulation environment and test cases were derived.

3. PROPOSED MECHANISM

A mechanism is being proposed to identify and prevent the wormhole attack using AOMDV protocol to transfer secure routing messages from the source sensor node and the destination sensor node. The first step is finding the route for communication. To start communication, the sensor nodes discovers its neighbors to route packets. This can be done by broadcasting a Route Request Packet (REQ). When the source receives the corresponding Route Reply Packet (REP), then it indicates that there is an availability of a route to the destination sensor node. If multiple Route Reply Packets (REP) are received then there is a possibility of more than one possible route to the destination node.

Once the route has been discovered, round-trip time (RTT) is computed at the sender node for all possible routes. By dividing the round trip time of each route by the corresponding hop count, the threshold round-trip time (RTT_{th}) is being computed. Compute the average threshold round trip time ($RTT_{avg\_th)}$ by dividing the RTT_{th} by the total number of paths to the destination. If RTT_{th} is less than RTT_{avg_th} and the hop count on established route equals two, then detect the route as a wormhole link.

Since the wormhole link has been discovered, the sender identifies w_s, the first node of the neighbor as the wormhole source node. Through neighbor w_s and established route, the sender sends the dummy route request packets (REQ). The destination node receives these dummy REQ packets from its neighbor w_d (neighbor node of the destination) and neighbor w_d is detected as the destination wormhole node by the receiver. Routing is restricted between w_s and w_d and routing entries are detached from the routing table and transmitted to other sensor nodes. This makes the wormhole affected link not to be used anymore and the link route is being jammed.

After a while, when the source node intends to communicate to that particular destination node, it verifies the routing table whether a route is already being established and also whether the corresponding route is affected by wormhole link. If the condition is being satisfied, then the corresponding route is discarded, and the source node chooses a route which is free for wormhole link from the routing list.

3.1 Proposed Algorithm

Two algorithms are being presented based on the proposed mechanism for wormhole detection and wormhole prevention. Algorithm 1 represents the wormhole detection algorithm. The inputs are the neighbor information and route discovery. The output will be the identification of the wormhole link. The source node broadcast REQ packet to identify the availability of path to the destination sensor node. If there is an availability of the route to the destination node, then the destination node in turn sends REP Packet to the source node. The round trip-time, threshold round-trip time and the average threshold round-trip time are calculated. From the calculated results, the wormhole affected route is being identified. After identification of the wormhole link, the procedure for wormhole prevention is executed. If the condition is not true, there is no possibility of wormhole attack.

Algorithm 1: Wormhole detection algorithm

1: **Input** Neighbor information,
Route discovery
2: **Output** Wormhole detection
3: **Begin** algorithm
4: **for** finding route
5: sender node broadcast Route Request Packet (REQ) at time t_q
6: sender nodes receives Route Reply Packet (REP) at time t_p
7: **end for**
8: Calculate Round Trip-Time (RTT)
9: $RTT = t_p - t_q$
10: Calculate Threshold Round-Trip Time (RTT_{th})
11: $RTT_{th} = (RTT / hopcount)$
12: Compute average threshold round-Trip Time (RTT_{avg_th})
13: **if** ($(RTT_{th}) < (RTT_{avg\_th})$) and (hop count on route == 2)
14: Detect the route as a wormhole link
15: do Prevention method
16: **else**
17: There is no possibility of wormhole attack
18: **end if**
19: **End** Algorithm

Algorithm 2 deals with the prevention algorithm of wormhole attack. The input to the algorithm is detection of wormhole and the output is secure data transmission between the source and the destination node.

Algorithm 2: Wormhole prevention algorithm

1: **Input** Wormhole detection
2: **Output** Secure data transmission
3: **Begin** algorithm
4: Sender detects w_s as the source wormhole node
5: Through w_s and established route, the sender sends the dummy REQ packet
6: The destination node receives these dummy REQ packets from its neighbor w_d
7: Neighbor w_d is detected as the destination wormhole node by the receiver
8: Routing is restricted between w_s and w_d
9: **End** algorithm

4. SIMULATION

A simulation scenario is being designed with fifty sensor nodes and the wormhole attack using AOMDV is simulated using NS2.35 simulator. The proposed simulation environment, parameters and scenario are briefly presented.

4.1 Simulation Environment

The simulation of wormhole attack incorporated with AOMDV protocol is simulated using NS2.35 on Ubuntu platform. The simulated traffic in the proposed simulation environment is CBR (Constant Bit Rate) traffic. The performance evaluation of the proposed AOMDV protocol is performed based on different network metrics such as End-to-End Delay, Packet Delivery Ratio, and Throughput.

4.2 Simulation Parameters

The various simulation parameters used for the proposed technique are shown in Table 1.

Table 1. Simulation Parameters

Parameters	Value
Simulation Area	500m x 500m
Proposed Protocol	AOMDV protocol
Simulator used	NS-2.35
Sensor nodes used	50
Channel Type	Wireless
Size of the Packet	512 bytes
Traffic Rate	CBR
Transmission Range	200m
Simulation Time	200s
Mobility Model	Fixed

4.3 Simulation Scenario

The simulation scenario for the identification of wormhole attack using AOMDV protocol in wireless sensor network is depicted in Figure 2. To identify or detect the wormhole link, the first step is to find the route for communication. This is accomplished by broadcasting Route Request Packet (REQ) and by receiving the corresponding Route Reply Packet (REP). If multiple Route Reply Packets(REP) are received then there is a possibility of more than one possible route to the destination node. Once the route has been discovered, round-trip time (RTT) is computed at the sender node for all possible routes. Then the threshold round-trip time (RTT_{th}) and the average threshold round trip time (RTT_{avg_th}) are calculated. If RTT_{th} is less than RTT_{avg_th} and the hop count on established route equals two, then detect the route as a wormhole link.

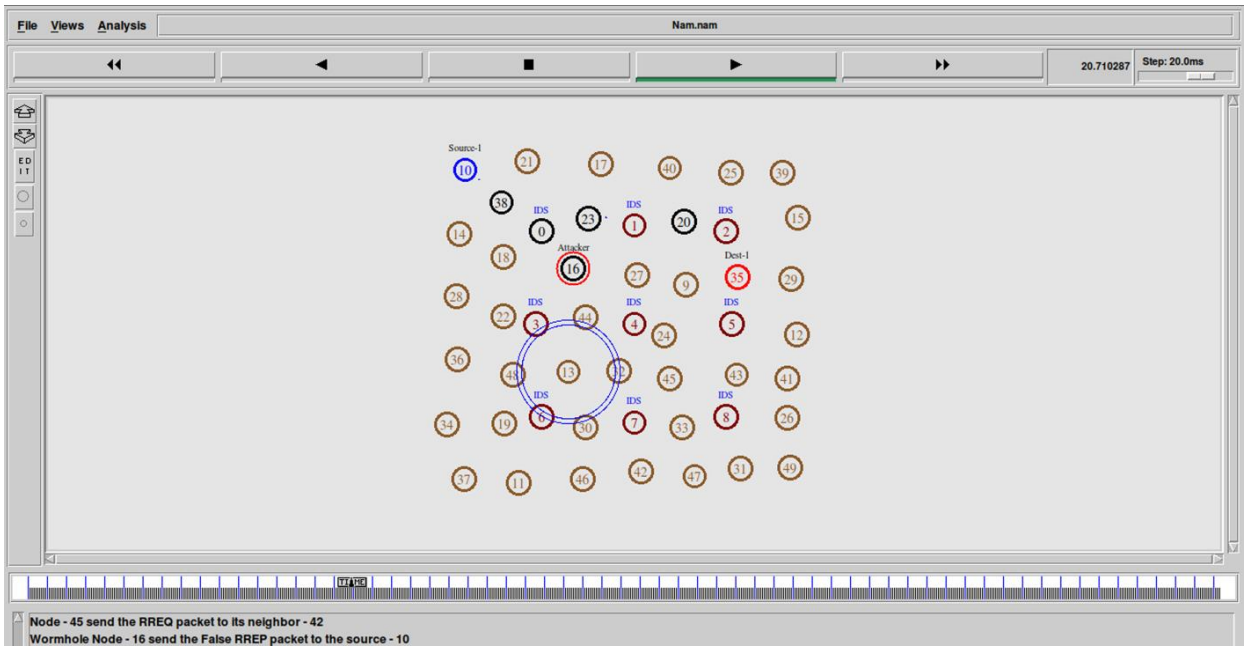

Fig 2: Simulation Scenario for detection of wormhole attack

The simulation scenario for the prevention of wormhole attack using AOMDV protocol in wireless sensor network is depicted in Figure 3. Since the wormhole link has been

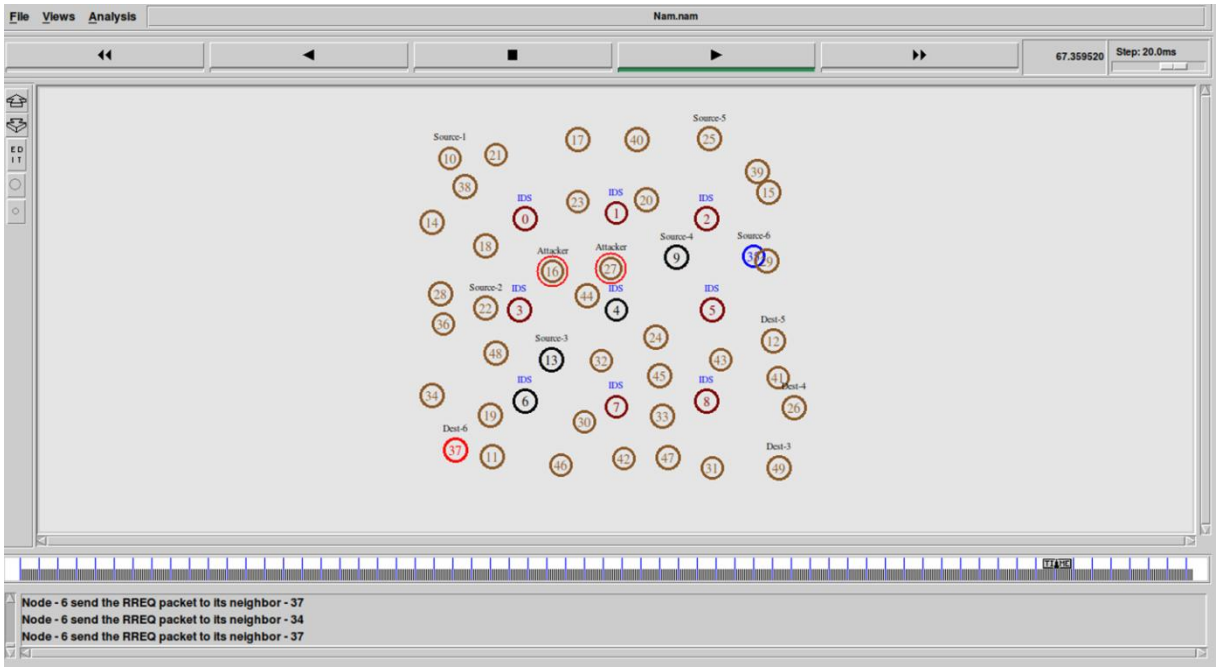

Fig 3: Simulation Scenario for prevention of wormhole attack

5. RESULTS AND DISCUSSION

Through neighbor w_s and established route, the sender sends the dummy route request packets (REQ)The destination node receives these dummy REQ packets from its neighbor w_d (neighbor node of the destination) and neighbor w_d is detected as the destination wormhole node by the receiver. Routing is restricted between w_s and w_d and routing entries are detached from the routing table and transmitted to other sensor nodes. This makes the wormhole affected link not to be used anymore and the link route is being jammed

The various performance metrics of AOMDV routing protocol is evaluated based on with or without wormhole attack on wireless sensor network. The performance metrics are based on End-to-End delay, Throughput and PDR (Packet Delivery Ratio).

5.1 End-to-End Delay

The end-to-end delay for the proposed mechanism is depicted in Figure 4. The x-axis represents the number of nodes and the y-axis represents the time at which the packet travels. End-to-End Delay is the time difference between the generated packet and the received packet. From the graph, it is identified that there is increase in the end-to-end delay with wormhole attack as compared to the attack without wormhole, due to multiple hop nature of the network.

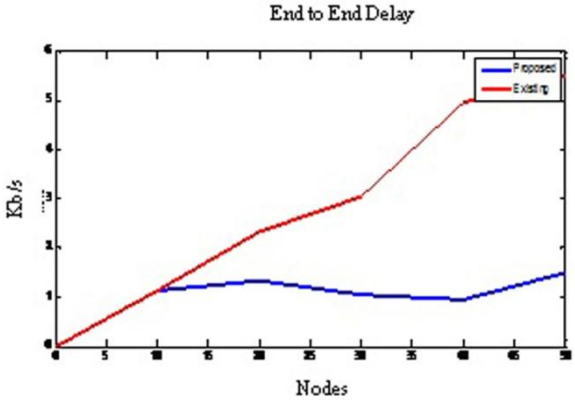

Fig 4: End-to-End Delay

5.2 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio for the proposed mechanism is depicted in Figure 5. The x-axis represents the number of nodes and the y-axis represents the number of packets. Based on the results of generated and received packets obtained from the trace file Packet Delivery Ratio (PDR) is calculated. PDR is the ratio of the received packets by the generated packets. From the graph, it is identified that there is decrease in the PDR with wormhole attack as compared to the PDR without wormhole.

5.3 Throughput

Throughput is calculated as the number of successful packets received in a unit time which is represented in bits per second (bps). The x-axis represents the number of nodes and the y-axis represents the time at which the packet travels. It is observed that the throughput decrease with wormhole attack in wireless sensor network as compared to without wormhole nodes. The throughput for the proposed mechanism is depicted in Figure 6.

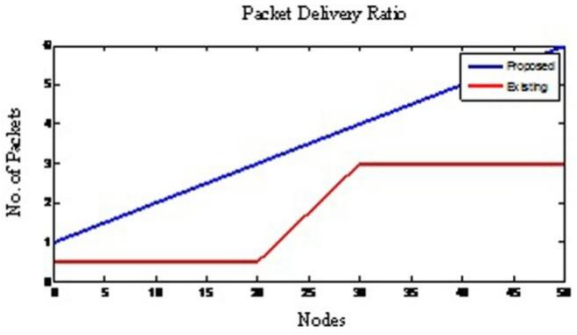

Fig 5: Packet Delivery Ratio

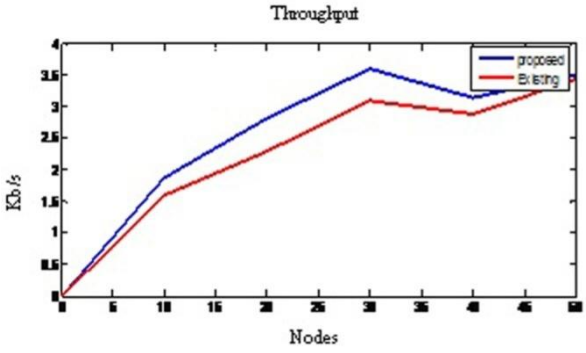

Fig 6: Throughput

6. CONCLUSION

Wormhole attack is considered as one of the network layer attack that need to be addressed in WSN. It is also considered the most hazardous attack in WSN. This paper deals with a mechanism to identify and prevent the wormhole attack by the process of route discovery. For this purpose Adhoc On-demand Multipath Distance Vector (AOMDV) protocol is being incorporated with the proposed technique. It calculates the round trip time (RTT) of every route which in turn calculates the threshold RTT. By this threshold RTT and the hop count information, the wormhole attack is being detected and prevented. The proposed technique is implemented using NS2.35 on Ubuntu platform. The simulated traffic in the proposed simulation environment is Constant Bit Rate (CBR). The performance evaluation of AOMDV protocol is computed based on different network performance metrics such as Packet Delivery Ratio, End-to-End Delay and Throughput. The simulation results shows that better performance is achieved in AOMDV proposed mechanism than wormhole affected AOMDV. This technique does not require any special hardware and is implemented with static mobility model. The future work will focus on designing dynamic mobility model and evaluation of other performance metrics.

7. REFERENCES

International Journal of Mobile Network Design and Innovation 8(1), 36 - 44.

[2] Orallo, E.H., Olmos, M.D.S., Cano, J.C., Calafate, C.T. and Manzoni, P. 2015. CoCoWa: A Collective Contact-

Based Watchdog for Detecting Selfish nodes. IEEE Transactions on Mobile Computing 14(2), 1162-1175.

[3] Nagar, J. and Sharma, S. 2015. K Barrier Coverage Based Intrusion Detection System for Wireless Networks. In the proceeding of 50th Golden Jubilee Annual Convention of Computer Society of India, 373-385.

[4] Buch, D. and Jinwala, D. 2011. Prevention of wormhole attack in Wireless Sensor Network. International Journal of Network Security & Its Applications (IJNSA) 3(5).

[5] Sharma, S., Mishra, R. and Singh, P. 2015. Authentication in Wireless Networks. In the proceeding of IEEE 2nd International Conference on Computing for Sustainable Global Development, 2031-2035.

[6] Murthy, C. S.R. and Manoj, B.S. 2017. Ad Hoc Wireless Networks-Architecture and Protocols. International Journal of Engineering and Advanced Technology 2(5).

[7] Akyildiz, I.F., Sankarasubramaniam, Y. and Cayirci,E. 2002. Wireless Sensor Networks : A survey. Computer Networks, Elsevier 38(4), 394-422.

[8] Ghazali, K.W.M. and Hassan, R. 2011. Flooding Distributed Denial of Service Attacks-A Review. Journal of Computer Science 7(8), 1218-1223.

[9] Jindal, S. and Maini, R. 2014. Comparative Analysis of Flooding and Jamming Attacks in Wireless Sensor Networks. International Journal of Engineering 3(4), 315-322.

[10] Manjula,V. and Chellappan, C. 2011. The Replication Attack in Wireless Sensor Networks: Analysis and Defenses. Advances in Networks and Communications 132, 169-178.

[11] Oh, S.H., Hong, C.O. and Choi, Y.H. 2012. A malicious and malfunctioning node detection scheme for wireless sensor networks. Wireless sensor network 4(3), 84-90.

[12] Goyal, A. 2014. Selective Packet Drop Attack in MANET-A Review. International Journal of Computer Science and Mobile Computing 3(5), 623-626 .

[13] Nithya, S. and Gomathy, C. 2018. An Investigation on Security Attacks in Wireless Sensor Network. International Journal of Pure and Applied Mathematics 119(15), 927-935.

[14] Dhama, S., Sharma, S. and Saini, M. 2016. Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks. In the proceeding of IEEE 3rd International Conference on Computing for Sustainable Global Development, 2993-2996.

[15] Sharma, S. and Mishra, R. 2014. A Cross Layer Approach for Intrusion Detection in MANETs 93(9), 34-41.

[16] Baadache, A. and Belmehdi, A. 2014. Struggling against simple and cooperative wormhole attacks in multi-hop wireless WSNs networks. Computer Networks 73, 173-184.

[17] Tomic, I. and McCann, J.A. 2017. Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. IEEE Internet of Things Journal 4(6), 1910 - 1923.

[18] Shanthi, S. and Rajan, E.G. 2016. Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks. International Conference on Next Generation Computing Technologies, 426 - 431.

[19] Sharma, S., Mishra, R. and Singh, K. 2013. A Review on Wireless Network Security. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer 115, 668–681.

[20] Qazi, S., Raad, R., Mu, Y. and Susilo, W. 2018. Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks. Journal of Information Security and Applications. Elsevier 39, 31–40.

[21] Shiu and Sheng, Y. 2011. Physical layer security in wireless networks: a tutorial. IEEE Wireless Communications 18(2), 66-74.

[22] Shree, R. and Khan, R.A. 2014. Wormhole Attack in Wireless Sensor Network. International Journal of Computer Networks and Communications Security 2 (1), 22-26.

[23] Amish, P. and Vaghela V.B. 2016. Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol. Procedia Computer Science, Elsevier 79, 700 – 707.

[24] Biradar, S.R., Majumder, K., Sarkar, S.K. and Biradar, P.S.R. 2010. Performance Evaluation and Comparison of AODV and AOMDV. International Journal on Computer Science and Engineering 2(2): 373-377.

[25] Chen, H., Lou, W., Wang , Z., Wu, J., Wan, Z., and Xia, A. 2015. Securing DV-Hop localization against wormhole attacks in wireless sensor networks. Pervasive and Mobile Computing, Elsevier 16, 22-35.

[26] Kumar,G., Rai, M.K. and Saha, R. 2017. Securing Range Free Localization against Wormhole Attack using Distance Estimation and Maximum Likelihood Estimation in Wireless Sensor Networks. Journal of Network and Computer Applications 99.

[27] Madria, S. and Yin, J. 2009. SeRWA: A secure routing protocol against wormhole attacks in sensor networks. Ad Hoc Net-works 7, 1051–1063.

[28] Bagade, S. and Raisinghani, V. 2016. Jitworm: Jitter monitoring based wormhole attack detection in manet. Information Systems Security, Springer, 444-458.

[29] Govindasamy,J. and Punniakody, S. 2017. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology.