Combating the Looping Behavior: A Result of Routing Layer Attack

David Samuel Bhatti[1], Kinza Sardar[2], Meh Jabeen[3], Umair B. Chaudhry[4]
[1, 2, 3, 4]Department of Computer Science and Information Technology,
University of Lahore,
Lahore, Pakistan
[1]School of Electrical Engineering and Computer Science,
National University of Science and Technology,
Islamabad, Pakistan

***Abstract*—Routing layer is one of the most important layers of the network stack. In wireless ad hoc networks, it becomes more significant because nodes act as relay nodes or routers in the network. This characteristic puts them at risk of routing attacks. A wormhole is the most treacherous attack on a routing layer of wireless ad hoc networks. The present proposed techniques require extra hardware, clock synchronization; or they make restrict assumption to deal with this attack. We have proposed a simple behavior-based approach which uses a small amount of memory for recording a few packets received and sent by the neighboring nodes. From this information, a behavior of these nodes is detected, that is, whether the behavior is benign or malicious. Nodes exhibiting malicious behavior are placed in the blocked node list. Malicious nodes are broadcasted in the network. None of the legal nodes in the network entertains any packet from these nodes. This approach has been simulated and verified in ns2.30 which detects and isolates wormhole nodes successfully. The current study focuses on the looping behavior of this attack.**

***Keywords*—Wormholes attack; wireless routing layer attack; detection time; throughput**

I. Introduction

Wireless ad hoc networks are very economical, simple and flexible. Easily, they can be deployed even in the hostile environments. Due to these features, they are being used extensively in civilian as well as in the defense domains. Their importance can be envisioned from the range of deployments; as they are deployed in large enterprise organizations, corporate sector, offices, and homes. Even, in the bodies of different living and non-living creatures like guided flying objects, these networks are operating now. Major categories of ad hoc networks are PANs, MANETs, VANETs and WSNs [1], [2].

But, now the wireless ad hoc networks are taking new turns and transforming themselves to Internet of Things [3], Internet of Vehicles [4] and mobile cloud computing [5]. With all these advantages, they are inherently broadcast networks and attract different types of attacks at different layers of the underlying network stack. The major attacks these networks encountering are the sinkhole, rushing, Byzantine, black hole, wormhole, and Sybil. Attacks like spoofing, dropping of routing traffic, selective forwarding, resource consumption are also important to be mentioned here [6], [7], [8], [9], [10], [11]. Besides this, the safe use of wireless devices like mobiles and smart-phones has been well discussed in [13]. All the attacks mentioned above are equally significant, but, the wormhole is one of the trickiest attacks observed in the literature [12]. The aim of this study is to devise a flexible and extendable mechanism to detect attacker nodes involved in the creation of wormhole link involved in looping of data packets.

In rest of the article, we have discussed wireless networks in Section II; routing protocols, wormhole attack and looping in Sections III, IV and V, respectively. Sections VI, VII and VIII shed light on wormhole classification, related work, and proposed approach. Under Sections IX, X, XI, results, future directions, and the conclusion is discussed.

II. Wireless Networks

This section has been added in this study to introduce the readers to different types of network and their applications; helping them focus on the particular type being discussed in this study.

A. Wireless Personal Area Network (PAN)

These are the networks which are within a reach of a person. These are the replacement of peripheral devices. NFC, Bluetooth, and Zigbee are the examples of such networks [46].

B. Wireless Local Area Network (LAN)

The range of this network can be campus, building, home or office. It is the extension of the wired network. WiFi (IEEE-802.11) types of networks fall into this category [46].

C. Wireless Metropolitan Area Network (MAN)

It's the type of network which covers an area of a city or a town. WiMax (IEEE 802.15) network are basically metropolitan area networks. They are used to connect wireless network with one another [46]. In other words, these provide inter-network connectivity.

D. Wireless Wide Area Network (WAN)

These are the big networks which provide wireless access beyond the range limits of LAN and MAN. LTE UMTS, GSM, and satellites networks all are the types of wide area networks [46]. The type of network discussed in this study

is basically an 802.11 WiFi ad hoc mode where no central control (Access Point) is applied rather the wireless nodes are providing relaying function themselves.

III. Routing Protocols

It has been observed that due to the ready availability of wireless technology, wireless networks are becoming very popular in all areas of life. Mobile ad hoc networks are among popular types of wireless networks have specific features like dynamic topology, open network boundaries and hop by hop communication. These networks are facing a lot of routing challenges too; some of these are the limited wireless range, constraints in battery power, heterogeneity in devices hardware and software, hidden terminals, etc.

Actually, it is the routing which finds and maintains routes between nodes, so that data can be transferred from the source to the destination. This process itself is considered to be the most challenging because nodes do not have familiarities with the underlying topology which is very dynamic in nature due to mobility. Messages are sent and received according to the predefined set of rules. These set of rules are referred to as protocols. Routing protocols are categorized into flat routing and geographical position assisted routing. In flat routing, each network identity is represented individually. Flat routing is divided into proactive, reactive and hierarchical/hybrid routing. Proactive routing protocols are also known as table driven routing protocols. DSDV, WAR, CGSR, WRP, QDRP, TBRPF, and OLSR are the well-known examples of proactive routing protocols [47], [48]. Whereas, AODV, DSR, LMR, TORA, and LQSR are the famous examples of reactive routing protocols [47], [48]. In proactive routing, the entire network routing information is maintained continuously by using the routing tables.

On the contrary, the reactive routing nodes only maintain information of the active routes to the destination nodes. In reactive routing searching for the path starts only when a node is required to send a data to another node in the network. In flat routing, wireless ad hoc networks start facing additional overhead when the network size increases. In these scenarios, hybrid/hierarchical routing protocols like ZRP, BGP, EIGRP, CGSR routing protocols are chosen [47], [48].

In the geographical position assisted routing, performance of the routing algorithm increases by using the moving node. Global positioning systems help in determining the location information of nodes in the network. LAR, DREAM, GPSR, and EGR are the protocols of geographical position assisted routing. Fig. 1 shows the taxonomy of these routing protocols [47], [48], [49].

In the current study, AODV has been used as a routing protocol in ns2.30.

IV. Wormhole Attack

Wormhole is one of the most problematic attacks in routing layer of the network stack [8]. It is a very intelligent attack that creates a tunnel whose one end opens at the sender side and other end opens at the receiver side.Whereas, these senders and receivers are very distant nodes. All traffic travels through this tunnel is controlled by the wormhole attackers. These attacker

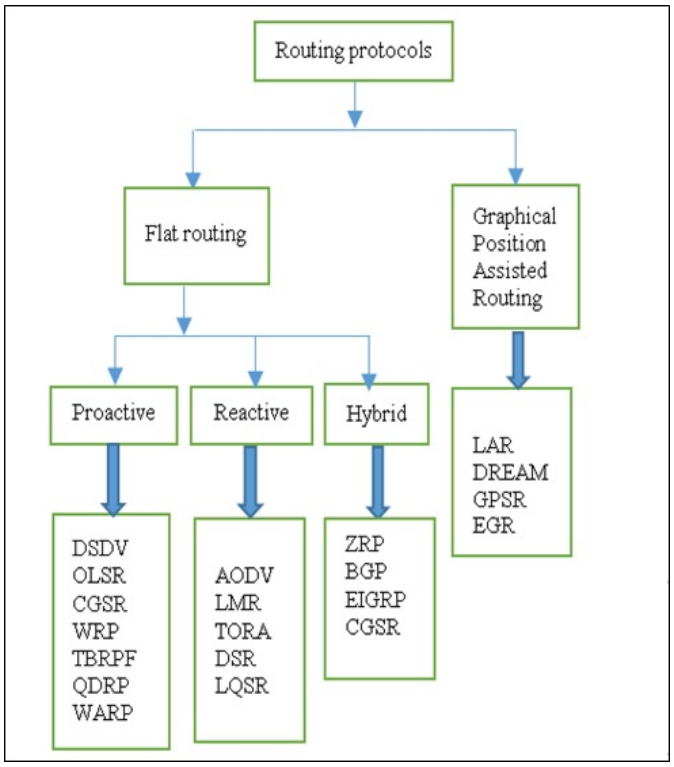

Fig. 1. Routing protocols in MANET.

nodes are sitting in the vicinity of sender and receiver which are many hops away from each other [10].

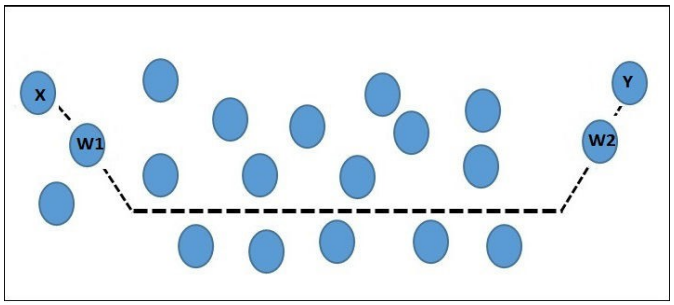

Fig. 2. Wormhole attack.

Usually, these attacker nodes have low latency wired or high radio range wireless link. This low latency link attracts the maximum traffic of the region covered by wormhole nodes. This is a 2 hops illusion created by wormhole which seduces the traffic to allure toward this malicious link in shortest path routing protocols. Wormhole captures traffic from one part of the network that is from sender side and replays it in another part of the network, that is, a receiver side. As shown in Fig.2, once the wormhole link has been established, wormhole node W1 captures the packets from the source X, relays them to the attacker node W2 which is resided in the vicinity of destination Y. Attackers W1 and W2 will take over the route X $\leftrightarrow$ W 1 $\leftrightarrow$ W 2 $\leftrightarrow$ Y.

When source will send data, this packet will be entrapped into a wormhole link W 1 $\leftrightarrow$ W 2. Due to, different malicious behaviors like replay and drop or loop-back of this link, a data

packet will not be able to escape from this trap. The scenario becomes worst when intermediate nodes are compromised they also start taking part in relaying traffic from one wormhole node to another. Wormhole can disrupt 30% to 90% of network [14]. Wormhole can also create sinkhole which result in the drawn of all traffic from the surrounding provided alternative routes are less attractive than the wormhole link [10]. State of the systems may become poor, when wormholes combine with Sybil attack, which becomes hard to detect then [11].

V. Looping Behavior of Wormhole

For the onward discussion we follow the conventions as given in Table I, as well as assuming, a wormhole link has already been established as shown in Fig. 2

TABLE I. Conventions to be Used

Node	IP-Address	MAC-Address
Source node "S"	IP-S	MAC-S
Destination node "D"	IP-D	MAC-D
Wormhole Attacker "W1"	IP-W1	MAC-W1
Wormhole Attacker "W2"	IP-W2	MAC-W2

In distance vector routing protocols, when the node "S" (Source Node) sends a data packet to "D" (destination node), "S" will insert its Source-IP "IP-S", Destination IP "IP-D" in place of Original-Src-IP and Original-Dest-IP, respectively. In the place of Src-MAC, it will insert its MAC "MAC-S" and in place of "Dst-MAC", it will place next node MAC "MAC-W1". "S" will transmit this packet. When this packet reaches the wormhole node "W1", then in the place of "Src-MAC", "W1" will insert its MAC "MAC-W1" and in place of "Dst-MAC", it will place next node MAC "MAC-W2". "W1" will transmit this packet through high radio range link established at route discovery time.

When this packet reaches the wormhole node "W2", then in the place of "Src-MAC", "W2" will insert its MAC "MAC-W2" and in place of "Dst-MAC", it will place "W1" MAC "MAC-W1". "W2" will change the direction of this packet while transmitting. This packet will come back to "W1". In this way, this packet not will reach the destination at all as shown in the Fig. 3. For the simplicity packets with fewer fields have been shown moving between two wormholes nodes W1 and "W2" in this figure.

VI. Classification of Wormholes Attacks

More robust solutions can be devised if the wormhole attacks are made classified according to their mode of behavior, that is, whether the attacker nodes are visible or not in the route. These are classified as open wormhole attack, closed wormhole attack, half open wormhole attack [50].

A. Open Wormhole Attack

In the open wormhole, source S, attacker X and Y and destination D are visible in the network. So, the path formed would be S↔X↔Y↔D. Attackers make themselves a part of the header following route discovery algorithm. A packet will be tunneled from one end to the other where it will be broadcasted. In this case, attackers do not let intermediate nodes A, B and C to make themselves visible in this network.

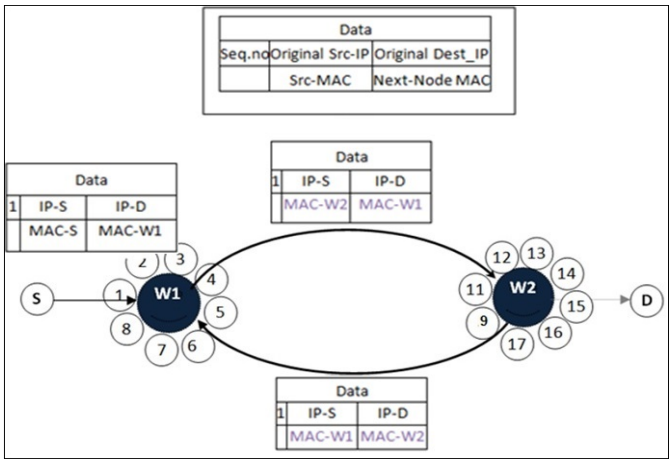

Fig. 3. Looping behavior of wormhole.

B. Closed Wormhole Attack

While in half open wormhole one of the attackers keeps itself hidden while other visible. Wormhole attacker close to the source will receive the packet from the source and will broadcast it in the other end. So the path formed would be S↔X↔D.

C. Half Open Wormhole Attack

Whereas, both of the malicious nodes X and Y nodes along with intermediate A, B and C are kept hidden in the closed wormhole. Source and destination think that they are one hop away from each other. Thus fake neighbors are created in this case. These three modes can be visualized from Fig. 4. Wormhole attacks can project themselves using packet encapsulation, high-quality/out-of-band link, high-power transmission capability, using packet relay and protocol distortion [50].

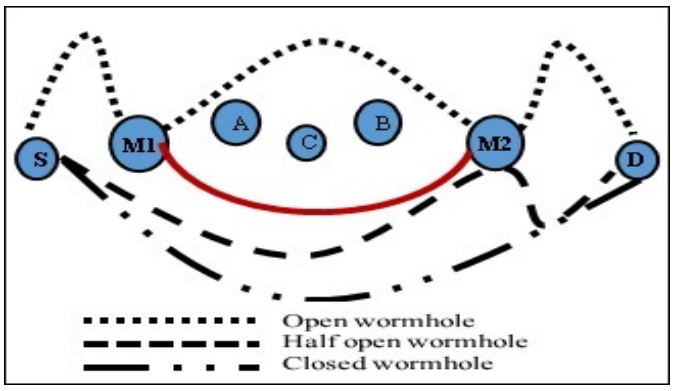

Fig. 4. Wormhole modes.

VII. Related Work

There are different types of mitigation approaches which have been discussed under different sections for the better understanding of the reader. They have been categorized like hardware-based, cryptographic-based, guard-node-based, packet-leashes-based, etc.

A. Reply Count-based Approaches

WARP [15] is a very promising approach for the mitigation of wormhole attacks. It is based on different abnormalities observed in the system. It modifies the RREQ message of AODV [17], [18], [19] protocol by introducing an additional field 'first-hop'. It adds three fields in AODV routing table named first-hop, RREP-count, and RREP-DEC-count. It uses an additional RREP-DEC message with the same fields as that of the RREP of AODV. 'Type' field of the RREP has been used to distinguish them. The addition of such fields in the packet header results in a considerable overhead of bandwidth. Upon receiving the RREP, originator always sends the RREP-DEC message. The routing table is also overwhelmed by storing the information of the first-hop, RREP-Count, RREP-DEC-count. Periodic broadcasts also result in the increase of bandwidth required. Nodes continuously observe the behavior of other nodes. If they notice some irregularities beyond a certain threshold, then these nodes will be cut off from the network.

DAWSEN [16] is a wormhole mitigation scheme which makes use of reply counts. DAWSEN is simple, but, requires a high power base station, so that, a request can be received in one hop.

B. Guard Nodes-based Approaches

Honey-pots are the computer nodes which are deployed in the network to attract the attackers, so that; they may be detected and kept isolated from the network. They are also used to study the unauthorized attempts to get access to different business information systems. Honey-pots have been proposed in [20] for catching wormhole nodes.

Authors in [20] suggest placing some honey-pot nodes with some vulnerability in the network. These honey-pot nodes will allure the attackers which become exposed ultimately and can be removed from the network subsequently. LITEWORP [21] is another approach which places guard nodes in the network to identify the wormhole nodes. These are simple approaches, but, in bigger networks, deployment of additional nodes may result in some scalability issues [22].

C. Cryptographic Approaches

Cryptographic approaches are husbanded with complex computational operations, but, still, some authors suggest them for the detection and isolation of wormhole links in wireless ad hoc networks.

Some of them are TESLA [27] "Timed Efficient Stream Loss-tolerant Authentication" and TIK [28] "TESLA with instant key", MOBIWORP [23], SOADV [24], SPINS [25], TrueLink [26], Ariadne [29], etc. These all approaches are computation and bandwidth hungry and some even require precise clock synchronization. For instance, TESLA, which cannot be achieved without additional dedicated hardware. TESLA [27] is good for laptop class, but, it does not suit network scenarios with low resources [25]. Since wormhole attack projects itself at the time of route discovery; so, it does not require cryptographic information to relay or forward routing packets. That is why; these approaches are still vulnerable to this attack [30].

D. Additional Hardware based Approaches

There are certain approaches which believe in, that there should not be any objection if some extra hardware is brought into use for the handling of this treacherous attack. Among these approaches [11], [31], [32] are the very famous one. They make use of the directional antenna. In these scenarios, receiver detects the direction of the signal and it can bypass the wormhole. But, all these scenarios put forward an assumption that sender and receiver must be carefully aligned with one another.

Moreover, [31] and [11] assume that secret keys are pre-shared and secure discovery of neighbor nodes is already running. Approach [31] can only partially mitigate the wormhole attack and scalability factor also rules out the use of such approaches according to other researchers [21], [26]. SECTOR [33], MOBIWORP [23], DAWSEN [16], Leashes [28] are some of the other approaches which fall in this category.

E. RF Based Techniques

Radio Frequency (RF) based approach has been proposed at the physical layer in [34]. A waveform with a special pattern is projected and if any of the wormhole nodes cause a change in this special pattern that can be detected easily, and, the route is discarded. This is fine where malicious nodes cause a change in the pattern, but, if they exactly replicate the wave form they can be bypassed [21]. It is also not feasible to provide every node with RF capability.

F. Hop-Count Based

The approach proposed in [36] suggests the pre-distribution of secret keys pairwise. According to them, secret keys can be generated by using the one-way hash functions. They also make use of a hop-count parameter to differentiate between normal and wormhole nodes. The approach proposed in [35] is fairly simple and based upon the number of hops traversed by the routing packet. In this approach, routes with a higher number of hops are considered to be fair, whereas, routes with relatively fewer hops are treated as the malicious or corrupted ones. This idea works well for high transmission-power based wormhole attackers, but, not equally suitable for low range attackers. Authors of [37] suggest detecting distant nodes whose messages arrive quite earlier than the messages sent by other nodes. This behavior predicts the suspiciousness of such nodes. These techniques are simple and free of extra hardware cost and complex cryptographic operations.

G. Graph Theory-based Approaches

Graph theory has been leveraged in this regard and approach [40], [44], [45] make use of this field for the detection and isolation of multiple occurrences of the wormholes. These are the more advanced versions of this attack which work together for projecting the collaborative attacks. These are new classes of attack; Evil Twin is one of the famous attacks of this category in wireless ad hoc networks.

H. Other Secure Routing Protocol Approaches

The authors of [38] make use of changes occurring in the network along with routing information to detect the

wormhole attacker nodes. It is a simple approach which does not require additional hardware and even does not impose any strict assumption. Secure routing protocols used in [8], [39]project a quite reasonable defense layer against the nodes which collude with one another for the launch of wormhole link. They achieve this by using end-to-end authentication with the help of hashed message authentication codes.

SEAD [41] is the secure routing protocol which provides authentication for routing processes. SEAD is basically an improvement of DSDV [42]. It is a good guard against attack which result in the modification of the packet, and hence unable to catch the wormhole nodes. In other words, it can only resist against the illegal increase in the sequence-no or illegal decrease in the hop-count. An approach proposed in [43], suggests to make use of Timed Colored Petri Net for the formal verification of the proposed approach, whether, the proposed approach works or not under different network conditions and scenarios. The technique in [43] is based upon the round trip time (RTT). The value of RTT is always very short over the routes with wormhole link and very high over the route which are free from this malicious link.

All these approaches are promising; each has its own pros and cons. The aim of this study is not to reject other proposed approaches but to bring attention of the research community toward simpler solutions, because they are equally as effective and efficient as compared to the complex solutions.

VIII. Proposed Approach

Referring to Section-V (Looping Behavior of Wormhole), data packets will not be able to escape from this wormhole. Neighbor nodes of both the attackers maintain suspicious-node-list by storing packet sequence-no, previous-hop and next-hop. If for the same packet, its previous hop is becoming its next hop and next hop is becoming its previous hop, then node will be suspected as wormhole attacker node. Neighbor nodes will send alert message for this node as suspicious node and a node on getting alerts beyond the certain threshhold, against this node, will broadcast the ID of this node as malicious. RERR message will be generated. On receiving RERR message, source sends new RREQ message, where the malicious nodes will be blocked to take part in new route discovery process. We have discussed the scenario where the tunnel is created with the help of compromised nodes in Fig. 5. In this case, W1 and W2 are real attackers whereas node-5 and node-11 are compromised nodes.

As an example, list of packets to be cached at node-1 has been shown in this figure. Nodes involved in looping can be detected from the cache list. If we look at the detection mechanism node-5 and node-11 will also be detected as malicious nodes and will be isolated.

Carefully, we have observed this event and decided to remove this limitation of isolation of compromised nodes in future. This whole mechanism has been formulated in the form of a flow chart given in 6, for the better understanding of the reader. Algorithm (Pseudo Code) which is close to implementation has been elaborated in Algorithm 1. For successful implementation of this algorithm, two cache lists were created one is the suspicious node list whose fields are packet-ID, previous hop, next hop and the other is blocked node list whose fields are malicious node-ID and witness-count. The purpose of the first list is to store the packets along with node-IDs and the purpose of the second list is to hold the malicious nodes Ids respectively. These lists are given in from Fig. 5 and 6.

Node Ids given in flowchart are ones used in the simulation, where ‘from’ and ‘to’ have been used for source-MAC and Destination-MAC, respectively. CBR is constant bit rate data traffic. Entries in the suspicious node list help to detect the looping behavior of malicious and compromised nodes. From Fig. 5 it can be observed that W1 is giving data packet to node-5, node-5 to node-11 and node node-11 to W2. W2 instead of delivering the packet to destination node “D” sends the packet back to node-11 and node-11 to node-5 and node-5 to W1. In this way, packets are kept in a loop until they drop down.

Detection algorithm processes the suspicious list and detects this behavior. Nodes showing this behavior are captured and are broadcasted in the whole network. Every node in the network on receiving broad alert against newly detected malicious node, adds that node in its list of blocked nodes. None of the nodes in the network accepts any route request packets from nodes placed in the blocked node list. This results in secure route discover.

IX. Results and Discussion

Simulations have been carried out in ns2.30 with 802.11 MAC, at 64 Kbps data rate, with an omnidirectional antenna, in 1000 m x 1000 m topology with 200 wireless legal and 2 wormhole nodes. In this simulation attacker nodes radio range is 400 m and legitimate nodes 80 m. Static as well as mobile scenarios with 1000 J as the initial energy of the nodes have been simulated for 5-100 seconds using AODV protocol. The packet size has been kept as 512 Bytes in all cases. The malicious behavior of the wormhole node-200 and node-201 referred in Fig. 7. In the absence of new scheme, these wormhole nodes capture data packets going from source node-34 to destination node-100. Wormhole nodes keep on relaying these data packets. Ultimately, their time to live (TTL)value reaches zero and they dropped down. Wormhole nodes can disrupt only selective packets just to make their detection more problematic.

When we apply the proposed approach, wormhole node-200 and node-201 were successfully detected and isolated. The new route discovered was free from wormhole attacker nodes. And a successful communication was made possible between the source node 34 and destination node-100 as shown in Fig. 7. Whereas, prior applying this new algorithm, the wormhole nodes did not allow the data packets to move from node-34 to node-100.

A. Throughput & Loss Ratio

The proposed approach has a quite satisfactory throughput, which has been observed ranging from 78% to 96%. In static scenarios, the average throughput was about 96%, whereas, in mobile scenarios, it was about 78%. These observations were made with two wormhole nodes. For brevity, results of one of the experiment have been shown in Fig. 8.

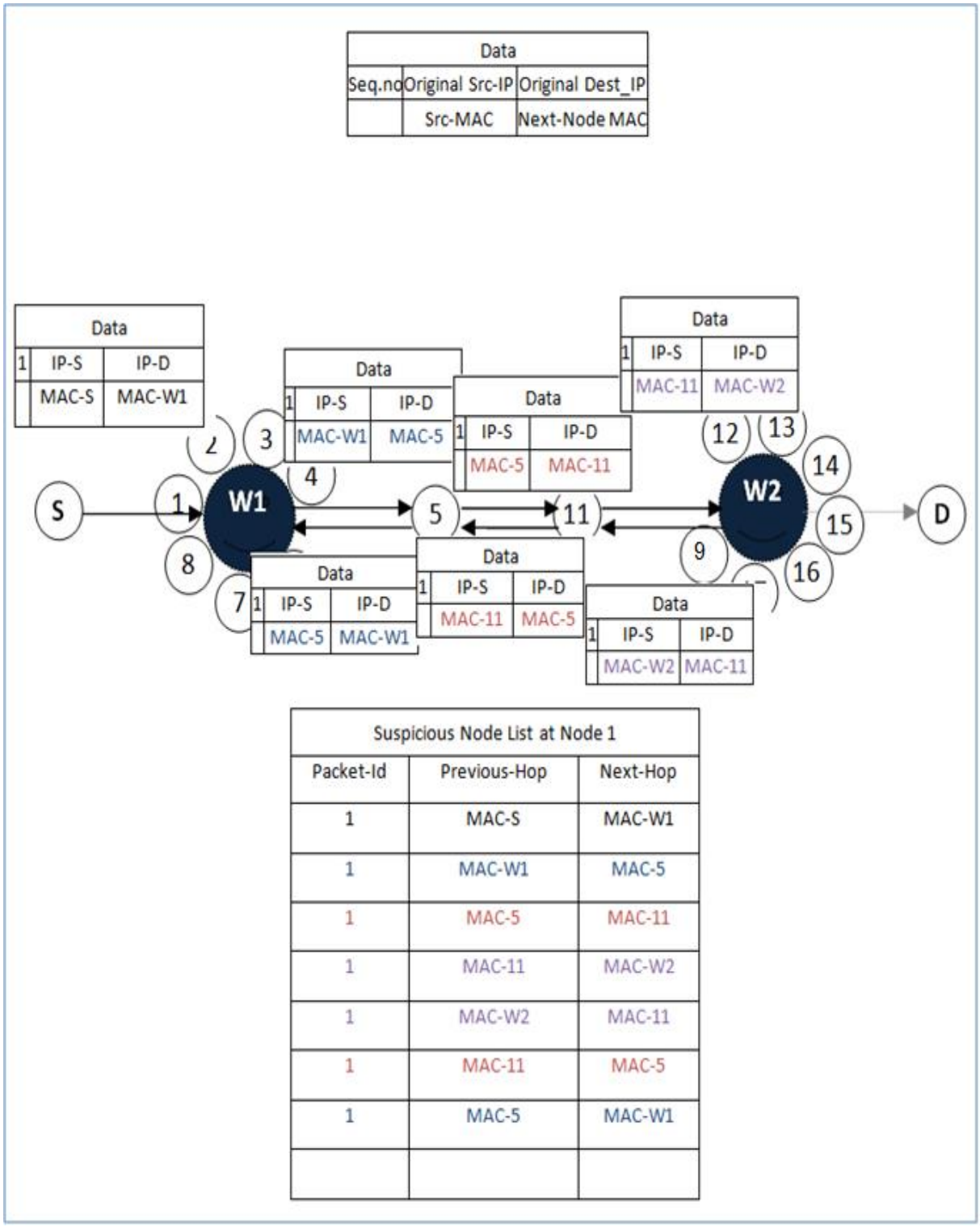

Fig. 5. Detection mechanism with intermediate node.

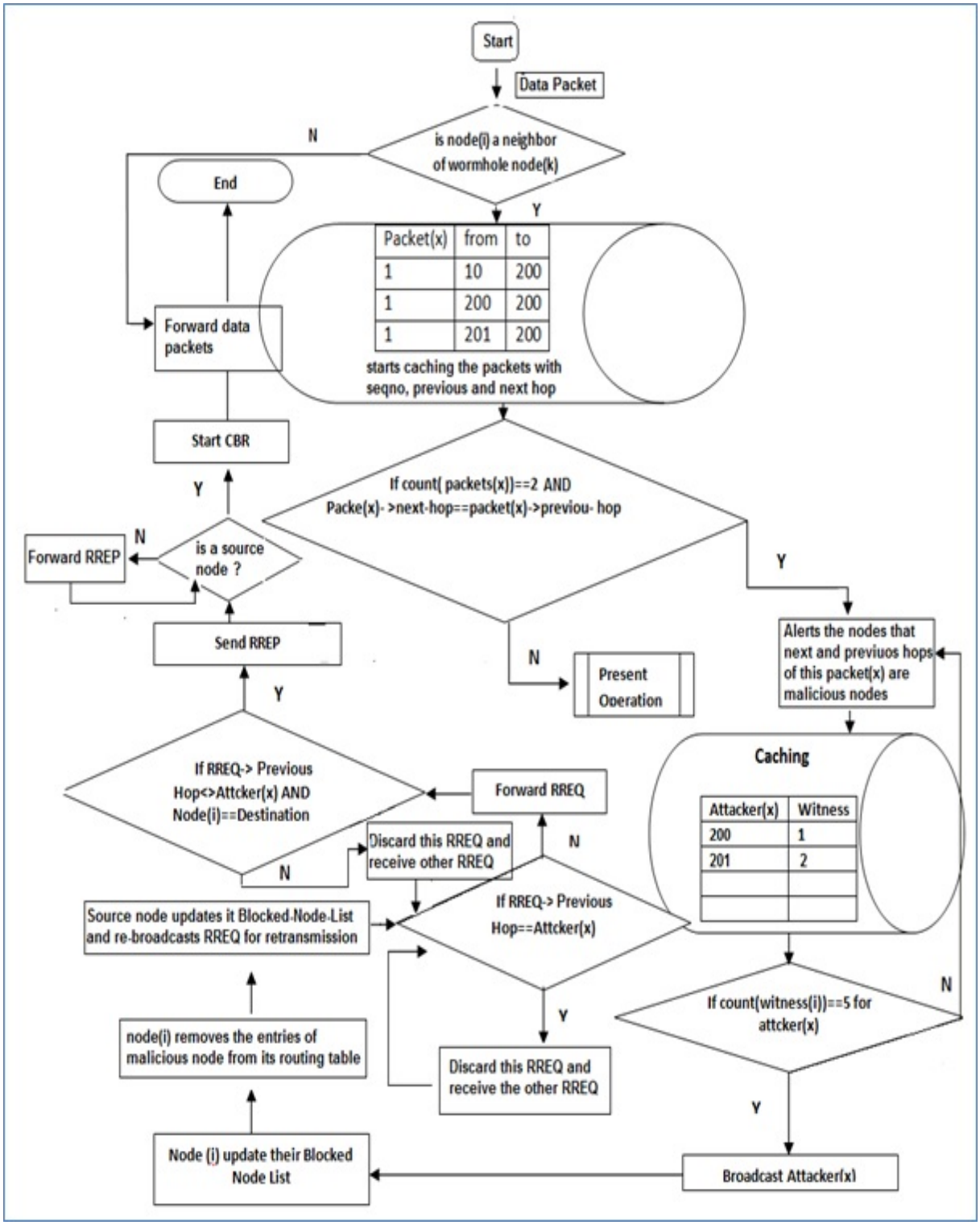

Fig. 6. Detection mechanism with intermediate node.

Algorithm 1: Wormhole Detection

```
begin
    if Packet Type = Data Packet then
        Store packet − id, previous − hop, next − hop in suspected neighbor list;
    else
        Forward Packet;
    end
    while NOT END OF "SuspectedNeighborList" do
        if same packet occurs twice whose next and previous hops are same then
            Generate 1 − hopalert against this suspected node;
    end
    Processing at Wormhole Neighbors
      The following operating will be performed
      at neighboring nodes wormhole
      1.Receive suspicious alert message
      2.Insert the suspected-nod in the blocked-node-list
      3.Increments witness-count
      Threshold of the witness-count is decided wisely
      if witness − count > Threshold then
        Broadcast this malicious node − idusingmaliciousalertmessage;
    Generate route error message;
    Processing at All Nodes
      All nodes will remove the entries of malicious nodes
      from their routing tables when they will receive the
      malicious node-id from malicious alert message.
      Moreover, nodes will update their blocked-node-list by
      adding this malicious node on receiving the malicious
      node-id
      Processing at Source Node
      Source node will broadcast RREQ again
      Processing at Intermediate Node
      Node Receive RREQ
      if RREQ previous − hop ∈ BlockedNodeList then
        DiscardtheRREQ;
    else if RREQ − destination − id = −node − id then
        Send RREP;
    else
        Forward the RREQ;
    Processing at Destination Node
      Node Receive RREQ if
      RREQprevious − hop ∈ BlockedNodeList then
        Discard the RREQ;
    else if RREQ − destination = node − id then
        send RREP;
    else
        Forward the RREQ;
    Processing at Source Node
      In this way, wormhole nodes will be filtered out
      because none of the nodes from the network will
      accept RREQ from the nodes listed in
      Blocked-Node-List. In this, there is very high
      probability the route established between source and
      destination will be free from the wormhole. Thus, the
      Source Node receives RREP from the path which has
      dispelled out wormhole nodes.It starts the
      retransmission of data packets. Data packet reaches a
      destination through newly established path
      successfully.
end
```

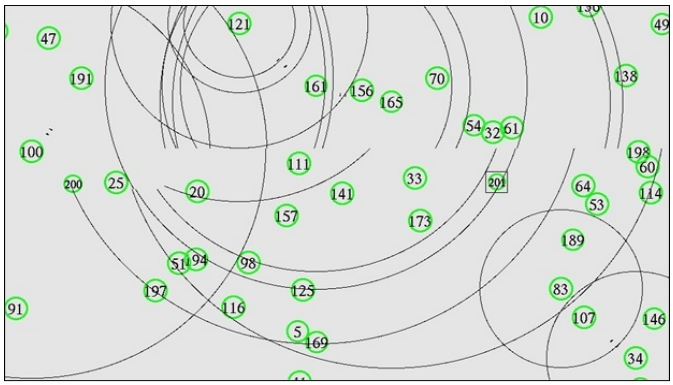

Fig. 7. Wormhole isolation in simulated environment.

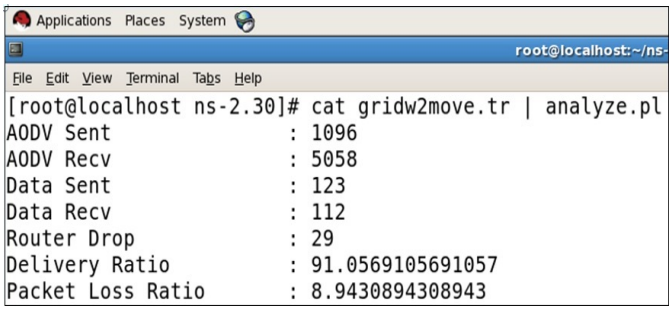

Fig. 8. Throughput in mobile scenario with 2 wormhole nodes.

B. Detection Time

Satisfactory detection and recovery time has been observed during the simulation. Simulation started at 1.0 second; wormhole nodes were detected at 1.149 seconds of the 10-100 second. It also depends upon the witness threshold. We suggest witness-count threshold to be kept low as one or two. However, if a witness-count threshold is kept low, detection latency will be decreased respectively. If it is kept high, detection latency would be increased, respectively. Therefore, it is important to wisely keep both the thresholds.

It was observed during simulation, the destination sends RREP at 1.248 second and data packets then successfully received at the destination at time 1.3150 second. Wormhole detection time, as well as system recovery time, is quite satisfactory. We calculated that system recovered within 0.15 second after the wormhole detection, as shown in Fig. 9

X. Future Work

We have planned to extend the existing approach for detecting multiple wormhole links equipped with other malicious behaviors like packet drop, packet selective drop, manipulation of TTL, replaying in wireless ad hoc networks. We aim that the extended strategy should be efficient with respect to memory, computation, and bandwidth.

XI. Conclusion

The proposed technique is simple, scalable and does not require any additional hardware. It does not impose any strict assumption of loose or tight clock synchronization for the proposed approach to work. The solution is not computation,

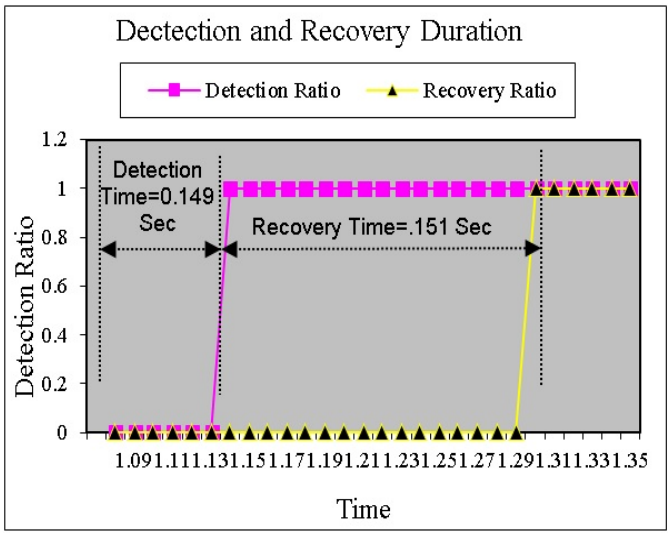

Fig. 9. Detection & recovery time.

memory, and bandwidth hungry. Size of cache lists is small enough to be easily processed by the wireless nodes including wireless sensor nodes. Thus, the solution is equally deliverable in small as well as in large wireless ad hoc networks in static as well as in mobile scenarios.

REFERENCES

[1] Y. Xiao and Y. Pan, "Emerging Wireless LANs, Wireless PANs, and Wireless MANs: IEEE 802.11, IEEE 802.15, 802.16 Wireless Standard Family," Wiley Publishing, 1st ed., 2009.

[2] I. Al Shourbaji, "An overview of wireless local area network (WLAN)," CoRR, vol. abs/1303.1882, 2013.

[3] M. A. Razzaque, M. Milojevic-Jevric, Palade, and S. Clarke, "Middleware for the internet of things: A survey," IEEE Internet of Things Journal, vol. 3, pp. 70-95, Feb 2016.

[4] J. Contreras-Castillo, S. Zeadally, and J. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security", IEEE Internet of Things Journal, vol. pp. 1-1, Apr 2017.

[5] L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, "Challenges on wireless heterogeneous networks for mobile cloud computing," IEEE Wireless Communications, vol. 20, pp. 34-44, Jul 2013.

[6] S. R. Surya and G. A. Magrica, "A survey on wireless networks attacks," in Computing and Communications Technologies (ICCCT), 2017 2nd International Conference on, (Chennai India), IEEE, 23-24 Feb. 2017.

[7] S. Mavoungou, G. Kaddoum, M. Taha, and Matar, "Survey on threats and attacks on mobile networks," Included in Special Section in IEEE Access: Security in Wireless Communications and Networking, vol. 4, pp. 4543 - 4572, August 2016.

[8] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in Proceedings of the SCS Communications Networks and Distributed Systems, Modeling and Simulation Conference (CNDS), (San Antonio, TX, USA), pp. 193-204, January 2002.

[9] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous secure routing in mobile ad-hoc networks," in Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, LCN 04, pp. 102- 108, 2004.

[10] C. Karlof and D. Wagner, "Secure routing in sensor networks: Attacks and countermeasures," in First IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003.

[11] L. Hu and D. Evan, "Using directional antennas to prevent wormhole attacks," in Proceedings of the IEEE Symposium on Network and Distributed System (NDSS), pp. 131-141, 2004.

[12] V. Kumar and R. Kumar, "Mitigation of wormhole attack using SOA in MANET," Global Journal of Pure and Applied Mathematics, vol. 13, no. 2, pp. 431-452, 2017

[13] D. S. Bhatti , N. A. Saqib, Z. Anwar," SCEAMS: Secure corporate environment adhered to mobile & smartphones", in 2016 Sixth International Conference on Innovative Computing Technology (INTECH), IEEE, Dublin Ireland, Aug.2016

[14] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," IEEE Transactions On Wireless Communications, vol. 8, no. 2, 2009.

[15] M.-Y. Su, "WARP: A wormhole avoidance routing protocol by anomaly detection in mobile ad hoc networks," Computer & Security, ELSEVIER, pp. 208-224, 2010.

[16] A. C. Z. D. Rouba El Kaissi, Ayman Kayssi, "DAWSEN: a defense mechanism against wormhole attacks in wireless sensor networks," in Second International Conference on Information Technology, (Dubai, UAE), 2005.

[17] C. E. Perkins and E. M. Royer, "Ad hoc on demand distance vector routing," in Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, WMCSA 99, 1999.

[18] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2003.

[19] C. E. Perkins and Belding-Royer, "Ad hoc on demand distance vector (AODV) routing," In IETF RFC 3561, (Mountain View, CA, USA), July 2003.

[20] P. V. T. Divya Sai Keerthi, "Locating the attacker of wormhole attack by using the honey pot," Liverpool, United Kingdom United Kingdom, pp. 1175-1180, 2012.

[21] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: Detection and isolation of the wormhole attack in static multi-hop wireless networks," Comput. Netw., vol. 51, pp. 3750-3772, Sep. 2007.

[22] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in Proceedings of the 2nd ACM Workshop on Wireless Security, WiSe 2003, (New York, NY, USA), pp. 30-40, ACM, 2003.

[23] I. Khalil, S. Bagchi, and N. B. Shroff, "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks," Ad Hoc Networks, vol. 6, no. 3, pp. 344-362, 2008.

[24] M. G. Zapata, "Secure ad hoc on- demand distance vector (SAODV) routing," in internet draft, Aug. 2001.

[25] A. Perrig, R. Szewwczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocol for sensor networks," in Mobile Computing and Networking, (Rome, Italy), 2001.

[26] J. Eriksson, S. V. Krishnamurthy, and Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proceedings of the 14th IEEE International Conference on Network Protocols, ICNP 2006, November 12-15, 2006, Santa Barbara, California, USA, pp. 75-84, 2006.

[27] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Tesla: Timed efficient stream loss tolerant authentication, broadcast authentication protocol," in CryptoBytes, pp. 2-13, 2002.

[28] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," vol. 24, (Piscataway, NJ, USA), pp. 370-380, IEEE Press, Sep. 2006.

[29] A. P. Y. Hu and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in MOBICOM, (Atlanta), pp. 12-23, ACM, September 2002.

[30] S. Choic, D. Kim, D. Lee, and J. Jung, "Wap: wormhole attack algorithm in MANETs," in 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung (Taiwan), 2008.

[31] Romit Roy Choudhury, Xue Yang, Ram Ramanathan, Nitin H. Vaidya, "Using directional antennas for medium access control in ad hoc networks", MobiCom '02, (New York, NY, USA), ACM, 2002.

[32] Y.-B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," in (INFOCOM) Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pp. 13-21, IEEE, 2000.

[33] S. Capkun, L. Buttyan, and J.-P. Hubaux, and E. M. Belding-Royer, "A secure routing Sector: Secure tracking of node encounters in multi-hop wireless networks," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN '03, New York, pp. 21-32, ACM, 2003.

[34] R. C. Merkle, "Protocols for public key cryptosystems," in Proc. of the IEEE Symposium on Security and Privacy, 1980.

[35] S.-M. Jen, C.-S. Laih, and W.-C. Kuo, "A hop count analysis scheme for avoiding wormhole attacks in MANETs," Sensors, vol. 9, no. 6, pp. 5022- 5039, 2009.

[36] A. S. M. E. A. G. M. K. K. X. L. Mehdi Sookhak, Adnan Akhundzada and X. Wang, "Geographic wormhole detection in wireless sensor networks," PLoS ONE, vol. 10, Jan 2015.

[37] H. Chen, W. Chen, Z. Wang, Z. Wang, and Y. Li, "Mobile beacon based wormhole attackers detection and positioning in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 10, no. 3, 2014.

[38] L. Lu, M. J. Hussain, G. Luo, and Z. Han, "PWORM: Passive and real-time wormhole detection scheme for WSNS," International Journal of Distributed Sensor Networks, vol. 11, no. 11, p. 356382, 2015.

[39] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields," protocol for ad hoc networks," in Proceedings of the 10th IEEE International Conference on Network Protocols, ICNP 02, pp. 78-89, 2002.

[40] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in INFOCOM 2007, 26th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, (Anchorage, Alaska, USA), pp. 107-115, May 2007.

[41] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, WMCSA 02, 2002.

[42] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers," in SIGCOMM Conference on Communication Architecture, Protocols, and Applications, ACM, 1994.

[43] L. Chen, C. Liu, and H. Huang, "Secure routing against wormhole attack and its formal verification based on timed colored petri net," in Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Q2SWinet '15, (New York, NY, USA), pp. 157-164, ACM, 2015.

[44] T. R. R. Revathi Venkataraman, M. Pushpalatha1 and R. Khemka, "A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks," International Journal of Recent Trends in Engineering, May 2009.

[45] L. A. Radha Poovendran, "A graph-theoretic framework for preventing the wormhole attack in wireless ad hoc networks," Wireless Networks (Springer), pp. 27-59, 2006

[46] Ilya Grigorik, "Introduction to Wireless Networks: Performance of Wireless Networks, Chapter 5", O'Reilly Media, Inc , 2013

[47] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011

[48] A. Chauhan and V. Sharma, "Review of performance analysis of different routing protocols in MANETs," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, pp. 541-545, 2016

[49] Harminder Kaur1, Harsukhpreet Singh, Anurag Sharma, "Geographic Routing Protocol: A Review", International Journal of Grid and Distributed Computing Vol. 9, No. 2, pp.245-254, 2016

[50] R. Mudgal and R. Gupta, "Study of various wormhole attack detection techniques in mobile ad hoc network," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, pp. 3748-3754, 2016