SRoWM: Smart Review on Wormhole Mitigation

David Samuel Bhatti[1], Shehla Saeed[2], Muhammad Asad Ullah[3], Naila Samar Naaz[4], Syed Saqib Raza Riz vi[5], Syed Taha Ali[6]

[1,2,3,4,5] Department of Computer Sciences and Information Technology, University of Lahore, Lahore, Pakistan
[6] School of Electrical Engineering and Computer Sciences, National University of Science and Technology, Islamabad, Pakistan

Summary
Wireless ad hoc networks getting rapid popularity and new domain like IOTs, IOVs, mobile cloud computing are asking for new security protocols for different layers of network stack. Network layer is one of the most important layers provided with routing function. Among various different attacks on routing, wormhole is the most treacherous one, which is possible without getting access of cryptographic information. The aim of this smart review is to explore wormhole mitigation techniques along with their strengths and limitations. This review will help the reader to design and develop new secure routing protocols for the new paradigms of wireless ad hoc networks.

Key Words
wormhole, RTT, RF, guard nodes, hop-count, MANETs, AODV, DSR, SEAD

1. Introduction

Due to, wireless ad hoc network's scalability, simplicity, flexibility, mobility and easy installation and deployment nature, they are getting rapid popularity in almost every scenario of human life. We find them wireless PAN, wireless LAN, wireless MAN, wireless WAN, mobile device networks etc [64][3]. Wireless networks are operating in open medium which inherently is a broadcast medium. They have a dynamic topology where the network operations are of distributed in nature with constrained capabilities. These are the reasons of these networks to be susceptible to different network threats. Security is considered to be a central requirement for these networks; since, the most important asset for any organization is its data which must be protected on priority basis. They are decentralized type of wireless networks and can be further categorized according to their application in different domains of human and machine activities.

Deployment of wireless networks varies from large organizations to living body. New domains of wireless networks are emerging such as Internet of Things[48], Internet of Vehicles[11] and Mobile Cloud Computing [29] , which also need to meet the latest security challenges. Some of the treacherous attacks on wireless ad hoc networks are sinkhole, rushing, byzantine, black holes, wormholes and sybil. Acknowledgement spoofing, dropping routing traffic, selective forwarding, resource consumption, HELLO flood, location disclosure, spoofed, altered and replayed routing information attacks are also very dangerous. These attacks have been well discussed in [56][33][38][67][22][13].

Among all above mentioned attacks wormhole is one of trickiest attack where two nodes collude each other to hack the routing information in wireless ad hoc networks. Wormhole in wireless networks can be of different categories such as opened, half opened, closed, encapsulation based, and can be launched using some out-of-band communication channel or using some low latency radio link with the help of high power transmission device [27]. This attack has also been discussed in a separate section. We aim to explore these and different other wormhole mitigation techniques.

Rest of the study has been organized as 2. wormhole attack, 3. wormhole modes, 4. wormhole mitigation approaches, 5. comparative view of mitigation approaches, 6. open challenge, 7. future work, 8. conclusion.

2. Wormhole Attack

Wormhole is a treacherous routing layer attack [38]. In this attack , the attacker tunnels messages that it receives in one part of the network and replay them in another part over a fast radio or wired link. The simplest form of wormhole is that when the attacker is a single node and has hosted itself between two other nodes. This attacker would not be forwarding packets between these nodes. However, wormhole attacks may involve two distance malicious nodes and can compromise neighbor nodes to make its launch successful [22]. In an operational network 30% to 90% of its communication can be affected badly by the wormhole with two attacker nodes [23]. One attacker resides usually in the neighborhood of the sender and other attacker resides in neighborhood of the receiver. These sender and receiver are usually many hops away from each other. The attackers may have wired connection

Manuscript received December 5, 2017
Manuscript revised December 20, 2017

or they may have low latency wireless radio link i.e. high radio range transmitter. Usually, attackers create an allusion of two hop distance between source and destination against rout request. If this is the most attractive rout; then link will allure all the traffic of their neighborhood. Once the wormhole has been established, attacker-X takes the packets from the source-A, send them to the attacker-Y, located nearby destination-B. Attacker-Y, which is close to the destination-B. Attackers X and Y will take over the route A ↔ X ↔ Y ↔ B as shown in Fig.1[47]. When source will send data, it will enter into wormhole link X ↔ Y but will not be able to escape from it due different malicious behaviors like replay, drop or loop-back etc. There might be intermediate nodes between two attackers called compromised nodes, which result in the formation of a tunnel of more than one hop. Wormhole can also create sinkhole which results in the drawn of all traffic from the surrounding provided alternative routes are less attractive than the wormhole link [22].

Scenario becomes worst, when wormhole combines with Sybil attack, they become hard to detect and then the severity level[13]. Unfortunately, standard on-demand routing protocols like DSR[21], AODV[39] as well as secure on-demand routing protocols like SEAD[16], Ariadne[65] and SRP [38][52] cannot avoid wormhole attack. Because this attack can be made successful by tunneling RREQ message through high quality channel that reaches earlier to destination than other requests, which will be accepted and RREP will sent by destination node. After that all the RREQ messages of same RREQ source, received later by destination node would be rejected [42][43]. So, in this way a wormhole link becomes established in the network.

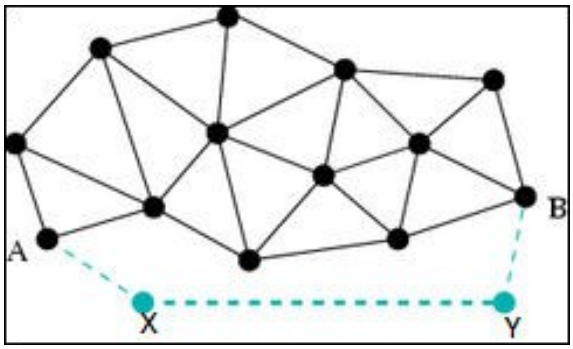

Fig. 1 Wormhole Attack

3. Modes of Wormhole Attacks

Wormhole attack is very critical to wireless ad hoc networks which depend upon shortest path routing protocols like AODV and DSR for route discovery and establishment. This attack can be projected in the different following modes, but, main aim of the attack remains the same, that is, to affect the maximum communication in the targeted network.

3.1 Encapsulation Based

In this mode, one of the attacker nodes encapsulates original RREQ packet into an additional capsule or an additional information header is wrapped around this original [37][60][34][19]. When this packet is reaches the second attacker nodes, it removes the additional header attached by first attacker node. A original packet is restored and and forwarded, which does not result in the increment of hop-count. When sink receives this packet it sends RREP message, and, a link becomes established containing the two wormholes nodes as well.

3.2 Packet Relay

The attackers are far away from each other, but, they give the illusion of being in the neighbor hoods of legal nodes through relaying packets between them [34][19].

3.3 High Transmission Power Based

This mode is projected when wormhole nodes possess high transmission power devices, through which they seduce the traffic of the neighboring nodes to be attracted, so that, traffic may reach faster to sink nodes[34][19].

3.4 Out of Band or High Quality Link Based

Fast wired or high quality wireless link can be used to launch this attack. RREQ reaches faster to sink using this link and the RREP is sent to source on the reversed rout which could be symmetric like in AODV. This link will be considered a shortest link by the legal nodes [34][19].

3.5 Protocol Deviation Based

In the standards of 802.11, nodes back off when one node is transmitting to avoid the collisions at MAC layer. But, wormhole attackers will not follow this rule and they keep transmitting during that period even, to corrupt the RREQ messages. Routing protocols which based upon the shortest delay rather than shortest hop will be affected badly [34][19].

4. Wormhole Mitigation Approaches

There are different types of mitigation approaches which have been discussed under different sections for better understanding of the reader.

4.1 Reply Count-based Approaches [55][50]

4.1.1 WARP [55]

WARP [55] capture wormhole attacker nodes on the basis of certain anomalies detected in networks. It modifies AODV [41][39] [43] RREQ message with additional field 'first-hop'. He added three fields in AODV routing table named first-hop, RREP-count and RREP-DEC-count. It has slightly high bandwidth overhead. He has used 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. Whenever the originator receives RREP, it sends the RREP-DEC message. WARP offers on the average 73% delivery ratio. There is an extra storage of information about first-hop, RREP-Count, RREP-DEC-count in routing table. In WARP, there is high bandwidth (communication) overhead of periodical broadcasts of Hello messages. Nodes keep on checking the anomaly values of their neighboring nodes regularly. If they find them with anomalies more than a certain thresh-hold, such nodes will be isolated.

4.1.2 DAWWSEN [50]

DAWWSEN [50] based upon reply counts. This scheme is simple, requires a high power base station where node will receive broadcast request in one hop.

4.2 Guard Nodes-based Approaches [57][24][51]

4.2.1 LITEWORP [24]

Honey-pots based scheme has been proposed in [57] for the detection of wormhole technique. In this technique a few nodes are designated as honey-pots and deployed in the network with some vulnerability. These nodes attract the attacker nodes and these malicious nodes are captured and removed from the network. It is simple, but, requires additional nodes.

LITEWORP [24] makes use of clock synchronization which needs extra hardware for the detection and prevention of wormhole. It is good, low cost solution for resource constraint environments.

It offers 98.9% non-malicious route isolation. However, the rate of missed detection increases when network becomes dense. Neighbor List, Watch Buffer and Alert Buffer have been used in this technique to implement mitigation of wormhole. LITEWORP [24] uses one-time authenticated neighbor discovery protocol and guard nodes. If wormhole attack launched itself successfully, before running of the neighbor discovery protocol, then this protocol can also be at risk to wormhole attack MOBIWORP [25]. LITEWORP [24] make use of clock synchronization and precise synchronization needs hardware implementation according to WARP [55]. Similarly, scalability factor of ad hoc networks rules out the use of clock synchronization and use of extra hardware [15].

4.3 CryptographicApproaches [25][2][28][66][44][12]

4.3.1 MOBIWORP[25]

MOBIWORP [25] is good approach towards the mitigation of wormhole attack but it is not suitable for resource-constrained environment because it is using public symmetric keys concept with Certification Authority (CA) implementation. Certification Authority (CA) storage capacity and its processing capabilities must be higher than the normal nodes. There is high overhead of bandwidth and processing for signature verification and authentication. Certification Authority (CA) is assisted by two other protocols Selfish Movement Protocol (SMP) and Connectivity Aided Protocol with Constant Velocity. MOBIWORP [25] incur a great overhead of computation for n-bit signature generation it requires $O(n^3)$ and verification $O(n^2)$. There is a great communication and bandwidth overhead for passing shared keys for verification. Storage overhead is visible from the lists maintained by MOBIWORP[25]. MOBIWORP[25] tries to remove the inefficiency of the LITEWORP [24] but needs the availability of location information Hu et al. [15] and is not suitable for resource-constrained environment.

4.3.2 Security Key [2]

There is data security key establishment using AODV proposed in [2]. This technique identifies different routing attacks like forged route reply, wrong routing information, interception. These attacks are handled by this approach. This approach assumes that there is a trust relationship between source and destination. This technique makes use of heavy and complex cryptographic functions for key generation, authentications and verifications. The wormhole can attack the target network without having access to the contents of routing packet header, even [10]. And this behavior makes its detection more challenging.

4.3.3 TESLA [45], TIK [17]

Some solutions impose complex calculations such as TESLA [45]"Timed Efficient Stream Loss-tolerant Authentication" and TIK [17] "TESLA with instant key". These approaches make use of complex cryptographic functions which incur high computational cost and communication overheads. TESLA [45] requires clock synchronization. Accurate clock synchronization needs

hardware implementation. TESLA [45] is good for laptop classes and internet applications but it does not suit the Ad hoc sensor networks which have limited storage and low processing power SPINS [44].

4.3.4 STM [28]

STM (Security Trust Monitor) [28] uses the trust values where 0 has been used for normal-trusted, 1 for misbehaving-untrusted, 2 for suspicious-untrusted and 3 has been used for malicious-untrusted. It is a good security design model which uses ”optimized link state routing protocol” OLSR as plugin. It is not suitable for resource constrained environment since OLSR incur high cost of signature generation and verifications of public key cryptography.

4.3.5 SAODV [66]

SOADV [66] is secure version of original AODV [41][42][43] used to secure the routing messages of AODV. SAODV uses digital signatures and hash chains. Digital signatures are used to authenticate non-alterable fields. Whereas, hash chains are used to authenticate alterable field, only the hop-count, in routing messages of AODV. It assumes that it has signature key pair and is well capable to verify the public keys of others. SAODV uses cryptographic functions [2], which ensure authenticity and integrity of routing messages. It also restricts the attacker to manipulate hop-count field of the RREQ and RREP messages. It also relies on the IPSec for the secure exchange of public keys [2]. Use of global computation is also not good for scalability of wireless ad hoc networks.

4.3.6 SPINS [44]

SPINS [44] implements security using two building blocks, ”Secure Network Encryption Protocol” SNEP and uTESLA[45]. SNEP provides confidentiality, data authentication, integrity and freshness. uTESLA authenticates broadcast messages. Secret keys are made shared for encryption and decryption between each node in the network and base station for both modules that is SNEP and uTesla.

SPINS makes use of heavy and complex cryptographic functions for the generation and verification of secret keys and this approach does not suit the resource-constrained environment. If TESLA Perrig et al. [45] is only suitable for internet applications.

4.3.7 TrueLink[12]

TrueLink [12] uses cryptographic functions and time synchronization to handle wormhole attack. This imposes computational complexity and reduces flexibility. The attackers with varying time delay can affect the results. Use of time synchronization is against the scalability feature of ad hoc networks.

4.3.8 Ariadne[65]

Ariadne [65] makes use of authenticated broadcasting technique by using symmetric cryptographic functions to achieve security goals against routing attacks. Basic requirement of Ariadne is that every node should possess an authentic element from the route discovery of each node initiating route discoveries along with public key. Public key cryptography imposes great overhead computation, caching and messaging with respect to resource constrained scenarios.

Still, these approaches are not saved from this treacherous attack, because wormhole can made launched successfully without having the information of cryptographic keys or even without having access to contents of the packet. Reason being is that they do not generate packets rather, use the existing packets over the network. Due to these capabilities wormhole attack becomes extremely problematic to handle because information inside the packet passing through wormhole remains unchanged [10] and use of clock synchronization, additional hardware and global computation affects the scalability feature of wireless ad hoc networks.

4.4 Additional Hardware Based Approaches[1][26][13][59][50][17]

4.4.1 Directional Antenna[1][26][13]

By using directional antenna [1][26][13] the receiver detects the direction of the signal and the wormhole can be prevented, but it puts the limitation that the sender and receiver must be carefully aligned along with antenna. Approach used in [1] based upon secure neighbor discovery, whereas, [13] impose that each node should share some secret keys with all other nodes, and this node has to maintain updated list of neighbors in a secure way. Due to the rigid approach to detect wormholes, degradation of network connectivity may happen. This means that some legitimate nodes may be isolated as wormhole nodes. Employing specialized hardware to mitigate the wormhole is not an economical and scalable approach if different scenarios of wireless network [12]. Directional antennas like [1] can only partially mitigate the wormhole [24].

4.4.2 SECTOR[59]

SECTOR [59] claims that wormhole can be detected with time synchronization. SECTOR makes use of ”Mutual

Authentication with Distance-Bounding" (MAD). Every node x sends one-bit challenge to every node y, then node y reply instantaneously. Thus, the distance from x-y is calculated. Using this flight time, node x determines whether, a node y is its neighbor or not. Shortcoming of this approach requires is this that it requires additional hardware that can manage this challenge request response husbanded with time measurements with high accuracy. Time of flight approaches are alike temporal leashes and they face the same limitation as that of the temporal leashes. This technique does not use cock synchronization but requires special hardware to support challenging request-response and for accurate time measurement MOBIWORP [25].

4.4.3 DAWSEN[50]

DAWSEN [50] requires powerful base station in form of additional hardware.

4.4.4 Leashes[17]

Leash is a piece of information, which is attached to packet to use it as a guard against the wormhole. TIK[17] based upon geographical and temporal leaches for capturing and isolating the wormhole nodes. Location based leash is called geographical leashes and the time-based leash is called temporal leash. Location-based leash requires location information of sender and receiver, requiring sender and receiver within certain distance from each other. This needs the nodes to know their location information and put the other limitation that all nodes should be timely synchronized. So geographical leashes need GPS and temporal leashes need clock synchronization [15]. The time-based leashes place the restrictions over the maximum distance a packet can travel. This approach put more strict restriction of tight time synchronization between all nodes.

These approaches ignore delay and packet processing times. Both approached add some information for authentication to each packet; this results in additional processing and communication cost LITEWORP [24]. In addition to this, the nodes need large amount of storage space at every node because they are using Merkle [36] like hash tree for authentication MOBIWORP [25]. Here in [36] authenticated distance bounding protocol named MAD has been employed. Similar to packet leashes, this approach is at higher level, not requiring GPS or clock synchronization, but, tolerates other inadequacies of packet leashes [15]. Geographical leashes call the Sybil attack where the attacker can represent it at more than one places. We cannot ignore the sending and receiving delay and packet processing time. In these approaches, the additional information is being added whose processing will take considerable amount of time. These approaches can face severe problems where contention based medium access control protocol is used. These techniques based upon spreading the HELLO messages where in-band wormhole does not require exchange of HELLO messages and can defeat such defenses [31]. Similarly, scalability factor of wireless ad hoc networks rule out the use of additional hardware [15]

4.5 Secure Localization Schemes [7][6]

Secure localization [6] [7] are very much suitable for the simplified network models where all network nodes have similar transmission power. Wormholes attackers can be detected under these systems very easily. Whereas in general models where the nodes have different ranges these schemes do not work well. Certain packets might be missed in these models due to collisions and the attacker can drop or overhear the packets randomly.

4.6 RF Based Techniques [36][53][54]

RF watermarking [36] is physical layer approach where the radio waveform is modulated in special pattern. If there is any change in the pattern, this triggers the detection of wormhole attackers. This can work well where the attackers are making some modifications. However, if they are exactly replicating the waveform then this solution fails in that case.

The approach proposed by Sastry et al. [53] uses fast radio frequency and relatively slow ultrasound signal to find the distance from time delay. Such approaches are appropriate only for selective range of beacons nodes, not possible to do this every node of the network system. Use of ultra-sound instead RF relaxes the use of time synchronization but needs additional hardware Hu et al. [15]. Techniques based upon radio frequencies fails to overcome wormhole attack if a wormhole nodes captures the waveform of radio signal accurately at receiving side, and then replicates it as it is at the transmitting LITEWORP [24]. To provide every node a RF capability is not economical and feasible ,and the approach may give birth to different scalability and compatibility issues [24].

4.7 Graph-Theoretic Algorithms[49][32][46]

Graph Theoretic approaches [49][46] have the capability to detect multiple wormhole working together in a collaboration. Approaches that use graph theory or geometry theory or link network connectivity information such as [32] result in the removal of legal nodes. In these graph-theoretic approaches, structure is drawn for network and the forbidden structures are detected and removed. Usually the guard nodes are specialized, trusted, higher ranged and need to know their location [15]. Wormhole mitigation technique proposed in [61] provides the

graphical support of existence of wormholes nodes in network. To do this, proposed scheme reconstructs the layout of the network with the help of multi-dimensional scaling. The approach can detect the wormhole and does not isolate the attacker nodes from the legal nodes [24].

4.8 Hop-Count, RTT Based, Cluster-based [20][58][35][5][51]

4.8.1 Hop-Count-Based [20][35]

Pairwise key pre-distribution approach has been proposed in [35]. One way hash functions have been used by the authors to generate public and private key pairs. Wormhole is detected from the hop-count values of the received message. This approach is simple and no extra hardware needed. Approach is free tight or loose clock synchronization and additional guard nodes.

The idea behind [20] is, that a user who does select routes with smaller hops can bypass the low latency link wormholes; because usually 5~6 hops a communication has to go through between sender and receiver. Whereas, wormhole link has very small hop-count, for instant two hops. However, the wormholes can go beyond two hop-counts. Similarly, if a malicious node is placed farther from the destination then malicious node route will be three greater hops than the legitimate rout. Therefore, if the route reply of greater hops has to be selected then it would be malicious route.

4.8.2 RTT-Based [58][51]

RTT (Round Trip Time) based approached [58] for wormhole attack detection has been implemented in three phases; neighbor list construction phase, route finding phase and wormhole attack detection phase.

Source stores RREQ time as well as intermediate nodes also stores RREQ forward time. When source receives its RREP against RREQ, it determines RTT vales of all intermediate, itself and destination. In case of no attack, values of all of these will be same. If RTT values will be too much high, there would be wormhole. This approach detects wormhole without use of any extra hardware for clock synchronization and cryptographic functions rather local clocks are used for synchronization. This scheme assumes that all the nodes have alike radio range, which implies that this scheme is not adequate when there are normal radio range wormhole attackers. This approach can face problems where the network connections change over time and congestion occurs frequently, since congestion can increase the delay time associated with a normal path, which will lead to high false alarm rate [10].

4.8.3 Cluster-based [5][51]

In cluster-based approach [5], authors have divided the entire network into three layers and every layer has its cluster head. Through the wormhole link, RREQ message arrive destination node faster and does not contain the Ids of cluster heads in its header as compare to RREQ message which follow legal path and containing the Ids of cluster heads in its header. It is assumed, that a wormhole link is a low latency link. RREQ messages not having the cluster heads Ids will not be entertained by the destination. This approach can handle only long radio range attackers. Another technique based upon the same feature as [5] is [4]

Barman et al. [51] have proposed a cluster-based algorithm for the detection of wormhole intrusion. This is based upon RTT concept where guard nodes are placed at inner layer. A guard node on finding the abnormal behavior for RTT by nodes, will report the cluster-head and the cluster-head will isolate those nodes as wormhole attackers. This is low cost solution, does not require any extra hardware and does not use complex cryptographic functions. For working of this scheme there are so many assumptions which need to be met e.g. network must be layered and there must be overlapping clusters, cluster membership is restricted to 2-hops, there must not be more than one cluster-head per cluster etc. we have to increase the number of guard nodes if want to increase the system performance. Use of guard nodes makes these approaches impractical due to scalability factor of the ad hoc networks. This is also impractical due to number of assumptions.

4.8.4 Mobile Beacon Based [8]

In this approach [8] wormhole nodes are detected and also their positioned is determined using geometric operations. The main idea used in this approach is to find farther nodes whose messages are received faster than the nearest nodes. This information along with topology information helps to locate the wormhole nodes. Technique is simple free from use of extra hardware, complex cryptographic functions etc.

4.9 Trust-Based Security for Wormhole Detection [18][63]

DSR [21] based [18] approach observes neighbor node behavior and records its trust level according to it. If the packet is dropped by node its trust level is decreased accordingly. This scheme prevents wormholes without the use of strict clock synchronization, cryptographic functions or additional hardware etc. In [63] trust-vector field has been created in the header. Wormhole uses the same packets header used by legitimates nodes. They do not generate new packets. An intelligent attacker can

easily modify the header field as they increase the sequence number. The solution may raise false alarms since the packets can be dropped at genuine node due to the low SNR, or due to weak medium or due to congestion etc.

4.10 Other SRP Approaches [30][38][52][32]

Topological based approaches like [30] uses just the routing information and variations occurring in network topology which helps detect the wormhole nodes in network. It is a simple approach and does not require extra hardware, clock synchronization, and cryptographic functions. Secure routing protocols [38][52] provides a good defence layer against attackers which does not collude. They achieve this using end-end authentication using hashed message authentication codes (HMAC) and disabling the routes caching. One-way hash chains are used by the SEAD [16] to provide authentication for the improved version DSDV [40]. It is guard against modification attacks, but, cannot deal with wormhole attack, which can be launched without modification of routing packet. It can only stop the attacker to increase the sequence-no or decrease the hop-count. Formally verified secure routing protocol has been proposed in [9], which employees the Timed Colored Petri Net for the formal verification of the scheme proposed scheme. In this technique wormhole detection is faster than the wormhole mitigation techniques based upon round trip time.

5. Comparative View of Mitigation Approaches

Different techniques for reducing the impact of wormhole attack have been studied. It has been seen that most of the techniques based on extra hardware employment, complex cryptographic functions, clock synchronization, or even strict assumptions. These mitigation techniques techniques have been compared and summarized in table 1 for the quick understanding of the the reader.

6. Open Challenges and Issues

i. Devising a simple scheme which must be free from extra hardware employment, complex cryptographic functions, and loose or tight clock synchronization is one the prime need for wireless ad hoc networks.
ii. New scheme must be extendable, scalable and suitable for resource constrained network environments with respect to memory, processing and bandwidth.
iii. Since wireless is broadcast medium, wormhole attackers broadcast data the same way as legitimate nodes. Then, how, a network's legal nodes instead of beating the attackers can leverage the tunnel created by using high quality link (wired link, long range radio link, high transmission power capability) for the faster transmission of network traffic from source to destination.

7. Future Work

We aim to develop security protocol for routing layer which must not use extra hardware, cryptographic functions, tight or loose time synchronization with minimum overheads of cashing, processing and messaging. The new technique must reduce the chances of isolation of legitimate nodes from the network.

8. Conclusion

Previous wormhole detection and removal techniques make use of cryptographic functions which impose computational complexity and reduce flexibility and where the communication of keys is also a big challenge. There are techniques which uses extra hardware which is also practically not feasible in every situation. Some schemes are based upon graph theory algorithms which also remove legitimate nodes. Some solutions are based upon tight and loose time synchronization where the attacker with certain delay and jitters can be synchronized with legitimate nodes and can be bypassed by the detection algorithms. Some used trust-based schemes which are not adequate as by certain change in attacker behavior; attacker can increase its trust level. Some added extra field in packet header which is not good security approach because wormhole attacker can manipulate the header as it uses the same packet since it does not generate any extra packet. So the mitigation of this attack with which eliminate all above reservation with minimum overheads of cashing, processing and messaging is a great challenge to research community.

References

[1] 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, 2002. ACM.
[2] Monis Akhlaq, M. Noman Jafri, A. Khan Muzammil and Baber Aslam "Data Security Key Establishment in AODV", in Proceedings of the 6th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications, pages 181-186. World Scientific and Engineering Academy and Society (WSEAS), 2007.
[3] Ibrahim Al Shourbaji, "An Overview of Wireless Local Area Network (WLAN)", CoRR, abs/1303.1882, 2013.

[4] J. Anju and C. N. Sminesh, “An Improved Clustering-Based Approach For Wormhole Attack Detection in MANET”, in Proceedings of the 2014 3rd International Conference on Eco-friendly Computing and Communication Systems, ICECCS ’14, pages 149-154, Washington, DC, USA, 2014. IEEE Computer Society.

[5] Subhashis Banerjee and Koushik Majumder, “Wormhole Attack Mitigation in MANETs: A Cluster Based Avoidance Technique”, International Journal of Computer Networks & Communications (IJCNC), 6(1):45–60, January 2014.

[6] H. Chen, W. Lou, X. Sun, and Z. Wang, “A Secure Localization Approach Against Wormhole Attacks Using Distance Consistency”, Eurasip Journal on Wireless Communications and Networking, Spatial Issue on Wireless Network Algorithms, Systems, and Applications, 2010.

[7] H. Chen, W. Lou, and Z. Wang, “Conflicting Set Based Wormhole Attack Resistant Localization in Wireless Sensor Networks”, in Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing, 2009.

[8] Honglong Chen, Wendong Chen, Zhibo Wang, Zhi Wang, and Yanjun Li, “Mobile Beacon Based Wormhole Attackers Detection And Positioning in Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, 10(3):910242, 2014.

[9] Lishi Chen, Chunyan Liu, and Hejiao 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, pages 157–164, New York, NY, USA, 2015. ACM.

[10] S. Choic, D. Kim, D. Lee, and J. Jung., “WAP: Wormhole Attack Algorithm in MANETs”, in IEEE 978-0-7695-315, 2008.

[11] Juan Contreras Castillo, Sherali Zeadally, and Juan Guerrero Ibaez “Internet of Vehicles: Architecture, Protocols, and Security”, IEEE Internet of Things Journal, PP(99):1–1, Apr 2017.

[12] Jakob Eriksson, Srikanth V. Krishnamurthy, and Michalis 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, pages 75–84, 2006.

[13] Linxuan Hu and David Evan, “Using Directional Antennas To Prevent Wormhole Attacks”, in Preceding of the IEEE Symposium on Network and distributed System(NDSS), pages 131–141, 2004.

[14] Y. C. Hu, A. Perrig, and D.B. Johnson. “Packet leashes: A defense against wormhole attacks in wireless networks”, in Proceedings of the 22nd INFOCOM, pages 1976–1986, 2003.

[15] Yi-Chun Hu, Adrian Perrig, and David 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, pages 30–40, New York, NY, USA, 2003. ACM.

[16] Yih-Chun Hu, David B. Johnson, and Adrian 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.

[17] Yih-Chun Hu, A. Perrig, and D. B. Johnson, “Wormhole Attacks In Wireless Networks”, volume 24, pages 370–380, Piscataway, NJ, USA, sep 2006. IEEE Press.

[18] [18] Shalini Jain and Satbir Jain, “Detection And Prevention Of Wormhole Attack In Mobile Adhoc Networks”, International Journal of Computer Theory and Engineering, 2(1):78, 2010.

[19] S. K. Jangir and N. Hemrajani, “A Comprehensive Review On Detection Of Wormhole Attack In MANET”, in 2016 International Conference on ICT in Business Industry Government (ICTBIG), pages 1–8, Nov 2016.

[20] Shang-Ming Jen, Chi-Sung Laih, and Wen-Chung Kuo, “A Hop-Count Analysis Scheme For Avoiding Wormhole Attacks In MANET”, Sensors, 9(6):5022–5039, 2009.

[21] D. Johnson, D. Maltz, and J. Broch, “DSR: The Dynamic Source Routing Protocol For Multihop Wireless Ad Hoc Networks”, Perkinson, ED. Edison-Wesley, 2001.

[22] C. Karlof and D. Wagner, “Secure Routing In Sensor Networks: Attacks And Counter Measures”, in First IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003.

[23] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, “Severity Analysis And Countermeasure For The Wormhole Attack In Wireless Ad Hoc Networks”, IEEE Transactions On Wireless Communications, 8(2), 2009.

[24] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, “LITEWORP: Detection And Isolation Of The Wormhole Attack In Static Multihop Wireless Networks”, Comput. Netw., 51(13):3750–3772, sep 2007.

[25] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, “MOBIWORP: Mitigation Of The Wormhole Attack In Mobile Multihop Wireless Networks”, Ad Hoc Networks, 6(3):344–362, 2008.

[26] Young-Bae Ko, Vinaychandra Shankarkumar, and Nitin H Vaidya, “Medium Access Control Protocols Using Directional Antennas In Ad Hoc Networks”, in INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, volume 1, pages 13–21. IEEE, 2000.

[27] Vimal Kumar and Rakesh Kumar, “Mitigation of Wormhole Attack Using SOA in MANETs”, Global Journal of Pure and Applied Mathematics, 13.

[28] Yannick Lacharit´e, Dang Quan Nguyen, Maoyu Wang, and Louise Lamont, “A Trust-Based Security Architecture For Tactical MANETs”, in Military Communications Conference, 2008. MILCOM 2008. IEEE, pages 1–7, Manchester Grand Hyatt San Diego, CA, USA, 2008. IEEE.

[29] Lei Lei, Zhangdui Zhong, Kan Zheng, Jiadi Chen, and Hanlin Meng, Challenges On Wireless Heterogeneous Networks For Mobile Cloud Computing”, IEEE Wireless Communications, 20(3):34–44, Jul 2013.

[30] Li Lu, Muhammad Jawad Hussain, Guoxing Luo, and Zhigang Han, “PWORM: Passive And Real-Time Wormhole Detection Scheme For WSNs”, International Journal of Distributed Sensor Networks, 11(11):356382, 2015.

[31] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis Of Wormhole Intrusion Attacks In MANETs”, in

Military Communications Conference, 2008. MILCOM 2008. IEEE, pages 1–7.IEEE, 2008.
[32] Ritesh Maheshwari, Jie Gao, and Samir 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, pages 107–115, Anchorage, Alaska, USA, May 2007.
[33] Silvre Mavoungou, Georges Kaddoum, Mostafa Taha, and Georges Matar, "Survey On Threats And Attacks On Mobile Networks", Included in Special Section in IEEE Access: Security in Wireless Communications and Networking, 4:4543 – 4572, August 2016.
[34] Dr. Zurina Bt Hanapi, Mehdi Enshaei, "A Review On Wormhole Attacks In MANETs", Journal of Theoretical and Applied Information Technology, 79(1):7–21, 2015.
[35] Mehdi Sookhak, Adnan Akhundzada, Alireza Sookhak, Mohammadreza Eslaminejad, Abdullah Gani, Muhammad Khurram Khan, Xiong Li and Xiaomin Wang, "Geographic Wormhole Detection In Wireless Sensor Networks", PLoS ONE, 10(1), jan 2015.
[36] Ralph C. Merkle, "Protocols For Public Key Cryptosystems", in Proc. of the IEEE Symposium on Security and Privacy, 1980.
[37] Farid Nait-Abdesselam, Brahim Bensaou, and Tarik Taleb, "Detecting And Avoiding Wormhole Attacks In Wireless Ad Hoc Networks", IEEE Communications Magazine, 46(4):127–133, 2008.
[38] P. Papadimitratos and Z.J. Haas, "Secure Routing For Mobile Ad Hoc Networks", in Proceedings of the SCS Commnication Networks and Distributed Systems, Modeling and Simulation Conference (CNDS), pages 193–204, San Antonio, TX, USA, January 2002.
[39] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", 2003.
[40] C.E Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequences Distance Vector Routing (DSDV) For Mobile Computers", in SIG COMM Conference on Communication Architecture, Protocols, and Applications. ACM, 1994.
[41] Charles E. Perkins and Elizabeth 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.
[42] Charles E. Perkins, Elizabeth M. Royer, and Samir R. Das, "Ad Hoc On-Demand Distance Vector Routing", IETF Draft, page 33 pages, October 1999.
[43] E. Perkins, C.; Belding-Royer, "Ad Hoc On-Demand Distance Vector (AODV) Routing" in IETF RFC 3561, Mountain View, CA, USA, July 2003.
[44] Perrig, R. Szewwczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocol For Sensor Networks", in Mobile Computing and Networking, Rome, Italy, 2001.
[45] Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Song, "TESLA: Timed Efficient Stream Loss Tolerant Authentication, Broadcast Authentication Protocol", in CryptoBytes, pages 2–13, 2002.
[46] Loukas Azoa Radha Poovendran, "A Graph Theoretic Framwork For Preventing The Wormhole Attack In Wireless Ad Hoc Neworks", Wireless Networks (Springer), pages 27–59, 2006.
[47] Daniele Raffo, "Security Schemes For The OLSR Protocol For Ad Hoc Networks", PhD thesis, Universit´e Pierre et Marie Curie-Paris VI, 2005.
[48] Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, and Siobhn Clarke, "Middleware for Internet of Things: A survey", IEEE Internet of Things Journal, vol. 3, pp. 70{95, Feb 2016.,
[49] T. Rama Rao Revathi Venkataraman, M. Pushpalatha and Rishav Khemka, "A Graph-Theoretic Algorithm For Detection Of Multiple Wormhole Attacks In Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, (2), May 2009.
[50] Ali Chehab Zaher Dawy Rouba El Kaissi, Ay-man Kayssi' "DAWSEN: A Defence Mechanism Against Wormhole Attacks In Wireless Sensor Networks", in Second International Conference in Information Technology, Dubai,UAE, 2005.
[51] Debdutta Barman Roy, Rituparna Chaki, and Nabendu Chaki. "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", CoRR, abs/1004.0587, 2010.
[52] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding Royer, "A Secure Routing Protocol For Ad Hoc Networks", in Proceedings of the 10th IEEE International Conference on Network Protocols, ICNP 02, pages 78–89, 2002.
[53] Naveen Sastry, Umesh Shankar, and David Wagner, "Secure Verification Of Location Claims", in Proceedings of the 2Nd ACM Workshop on Wireless Security, WiSe '03, pages 1–10, 2003.
[54] Ronggong Song, Peter C. Mason, and Ming Li, "Enhancement Of Frequency-Based Wormhole Attack Detection", in 2011 IEEE Military Communications Conference, Baltimore, MD, USA, November 7-10, 2011, pages 1139–1145, 2011.
[55] Ming-Yang Su, "WARP: A Wormhole Avoidance Routing Protocol By Anomaly Detection In Mobile Adhoc Networks", Computer & Security, ELSEVIER, pages 208–224, 2010.
[56] S. R. Surya and G. Adiline Magrica, "A Survey On Wireless Networks Attacks", in Computing and Communications Technologies (ICCCT), 2017 2nd International Conference on, Chennai India, 23-24 Feb. 2017. IEEE.
[57] Pallapa Venkataram T. Divya Sai Keerthi, "Locating The Attacker Of Wormhole Attack By Using The Honeypot", pages 1175–1180, Liverpool, United Kingdom United Kingdom, 2012.
[58] Zaw Tun and Aung Htein Maw, "Wormhole Attack Detection In Wireless Sensor Networks", World Academy of Science, Engineering and Technology; International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 2(10), 2008.
[59] S. Capkun, L. Buttyan, and J. P. Hubaux, "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, pages 21–32, New York, NY, USA, 2003. ACM.
[60] Paulo Verissimo, "Travelling Through Wormholes: A New Look At Distributed Systems Models", SIGACT News, 37(1):66–81, 2006.

[61] W. Wang and B. Bhargava, "Visualization Of Wormholes In Sensor Networks", in Proceedings of the 2004 ACM workshop on Wireless security (Wise), pages 51–60, 2004.
[62] Weichao Wang, Bharat Bhargava, Yi Lu, and Xiaoxin Wu, Defending Against Wormhole Attack In Mobile Adhoc Networks", Journal of Wireless Communication and Mobile Computing, 6(4), June 2006.
[63] Khin Sandar Win, "Analysis Of Detecting Wormhole Attack In Wireless Networks", World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 2(12):2704–2710, 2008.
[64] Yang Xiao and Yi Pan, "Emerging Wireless LANs, Wireless PANs, and Wireless MANs: IEEE 802.11, IEEE 802.15, 802.16 Wireless Standard Family", Wiley Publishing, 1st edition, 2009.
[65] Perrig Y. Hu and D. Johnson, "ARIADNE: A Secure On-Demand Routing Protocol For Ad Hoc Networks", in Mobicom, pages 12–23, Atlanta, September 2002. ACM.
[66] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing", in INERNET DRAFT, Aug. 2001.
[67] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, and Robert 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, pages 102–108, 2004.

Table 1: Comparison of Secret Key Generation Techniques

Sr	Method	Requirement	Commentary
1	Topology variation based [30]	No special requirements, needs only routing information	Does not require extra hardware, cryptographic function, loose or tight synchronization
2	Hop-Count, RTT Based Approaches and Cluster-based [20] [58] [35] [5][51]	Assumes all nodes have same radio range	fails where connection changes over time and congestion occurs frequently [10]
3	RFBased [54][53]	Timing requirement, additional Hardware	Fail to prevent wormhole when attacker replicated waveform also infeasible to mount this capability on all nodes[24],scalability factor rules the use of additional hardware, clock synchronization[15],
4	Packet leashes, geographical[14]	Location information; loose clock synchronization (ms)	it is simple and robust approach; suffers adequacies of GPS systems[63]
5	Packet leashes, Temporal[17]	Tightly synchronized clocks (ns)	it requires clock to tightly synchronized which is not attainable in WSNs presently [63]
6	Packet leashes, end-to-end[62]	GPS coordinates; Loosely synchronized clocks (ms)	Inherits limitations of GPS technology[63]
7	Time of flight[59][15]	one-bit message enabled hardware component which can generate quick response bypassing CPU	not compatible with existing MAC-layer, modification may require at this layer , use Cryptographic Hash Functions[63], scalability factor rules the use of such scheme[15], may not be feasible for typical wireless scenario[12]
8	Directional Antennas[1][13]	every node should have directional antenna capability nodes beside the GPS a	suitable for devices already employed directional antennas, not suitable to every scenario of the network
9	STM[28]	Needs OLSR as Plug-in	OLSR itself is complex cryptographic functions, high cost signature, generation and verification
10	Localization[7][7][6]	Location-aware guard Nodes	Good solution for sensor networks , suitable for networks with similar radio ranges[63],not readily applicable to mobile networks[63], scalability issue rules the use of guard nodes[15]
11	LiteWorp[24]	Clock Synchronization	Applicable only to static stationary networks[63], neighbor discovery process is vulnerable to wormhole attack[15], scalability issue[15]
12	MOBIWORP[25], TrueLink[12], SAODV[66],SPINS[44], TESLA[45], TIK[17],SRP[38][52], DSDV[40]	Cryptographic Keys concept with CA , Synchronization	Not suitable for resource-constraints environment[63] ,scalability feature rules the use of additional hardware, guard nodes, cryptographic functions, clock synchronization, global computation(CA) etc[15], Wormhole attack can be made possible without having knowing the encryption decryption keys keys[1]
13	WARP[55]	no requirements	Good solution for ad hoc networks with slightly low delivery performance, and have a high packet loss ratio