Evaluating the Research Trends and Techniques for Addressing Wormhole Attack in MANET

S.B. Geetha
Dept of Computer Engineering
MMCOE, Pune, India

Venkanagouda C Patil, Ph.D.
Department of E and CE
BITM, Bellary, India

ABSTRACT
Security issues in mobile adhoc network (MANET) are veiled by various techniques that were introduced in past decade. Owing to decentralized nature of MANET, the security issues cultivates resulting in welcoming various lethal vulnerabilities. Out of all security issues in MANET, wormhole attack is considered one of the most challenging adversarial modules that tremendously affect the communication system in MANET. This paper presents various significant security techniques for mitigating wormhole attack in MANET. The uniqueness of this paper is that it presents a state-of-art study of existing survey papers and potentially emphasized on techniques for detection and prevention of wormhole attack in MANET. Finally, the study also highlights some of the significant findings as well as research gap that stand as prime contribution of the proposed paper.

Keywords
Mobile Adhoc Network, Security, Wormhole Attack, Wormhole Tunnel.

1. INTRODUCTION
In the area of mobile communication technology, mobile adhoc network is one of the most discussed topics among the research community. A Mobile Adhoc Network (commonly known as MANET) consists of group of mobile nodes that are free from any network infrastructure [1]. The prime purpose of MANET is to ensure that user could access the resources in mobility. However, this is the root cause of all the problems in MANET. MANET is characterized by dynamic topology for which reason it the mobile nodes moves in random movement and it is not possible to assume the next point of mobility. Owing to this dynamic topology, the mobile nodes in MANET need to ensure that their routing is highly stabilized as with the movement of nodes, possibility of intermittent links increases. This phenomenon will also mean that a mobile node will need to perform consistent listening mode with other nodes and need regular update of routing tables. Hence, a huge amount of energy is drained out causing the node to degrade its performance slowly affecting the network performance. Therefore, it can be seen that MANET has lots of interconnected issues e.g. energy drainage, intermittent or unstabilized links, routing, bandwidth consumption, latency, inter-arrival time etc [2]. In more than past decade, there are bundle of significant research attempts, where majority of the focus was laid on to the design and enhancement of the routing protocols. Although, there are many routing protocols in MANET [3], but 98% of the studies till date are only focused on routing protocols viz. AODV (Adhoc On-Demand Distance vector), DSDV (Destination Sequence Distance Vector), DSR (Dynamic Source Routing), and OLSR (Optimized Link State Routing) mainly. All these routing protocols have their own advantages and disadvantages that motivate the researchers to either enhance these routing protocols or design a new one. Apart from the performance issue in MANET, security is another unsolved issue among the research group. Some of the recent studies like [4][5][6] have already discussed various security threats as well as the possible mitigation technique evolved till date. Various type of security threats (or attacks) investigated till date are known to be black hole attack, spoofing, sinkhole attack, Sybil attack, packet dropping, rushing attack, cloning attack, flooding (or Denial-of-Service) attack etc. Out of all these security threats, wormhole attack is one of the most frequently used research topic, where inspite of various mitigation techniques being surfaced in the past studies, till the security systems on MANET are shrouded by the vulnerabilities of wormhole attack owing to their invisible tunneling phenomenon [7].

Hence, a curiosity being raised that why the techniques and algorithms being discussed till date are not able to solve the vulnerabilities of wormhole attack. Therefore, this fact has inspired us to carry out an in-depth investigation to understand the effectiveness of the prior techniques so that it can assist the future researcher to design their mitigation technique more effectively. The work done for this paper has closely observed and investigated about various factors, issues, parameters, and techniques adopted till date and finally the study discusses about the open issues (or research gap) for the techniques being presented in prior studies till date. As there are already survey papers on attacks on MANET available that has more and more theoretical and repetitive discussion; the core findings of the study have been highlighted here and the theoretical discussion about domain has been avoided in this paper. Section II will brief about the base of the wormhole attach in MANET followed by Need of the study in Section III. Section IV discusses about the existing survey works followed by Section V that discusses about the existing techniques of mitigating wormhole attacks in MANET focusing on the exclusive analysis of the techniques, parameters adopted, and effectiveness of the outcomes. Section VI highlights the research gap, while Section VII makes some concluding remarks.

2. WORMHOLE ATTACK IN MANET
Wormhole attack is one the most lethal attack among the various other types of security vulnerabilities in mobile adhoc networks. In such type of attack, an adversary captures the data packet from one mobile node and routes them to another node in the network. Such routing is also called a tunneling process in wormhole attack [8]. Interesting point to note is that when the adversary performs tunneling the captured message, the compromised packet arrives at the destination node much speedily even before the arrival of the original data packet from the regular user. Usually, such wormhole tunnels as well as adversarial nodes are completely invisible in the network causing many challenges to the network and security engineers. If the tunneling distance is longer

compared to the usual transmission range of a single hop network, the process of invoking an attack becomes simpler for the malicious node. A simpler version of wormhole attack is shown in Fig.1.

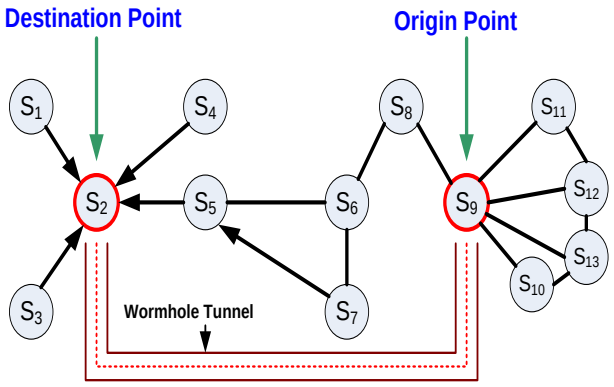

Fig 1: Scenario of Wormhole Attack in MANET

In the above schematic representation (Fig.1), it can be seen that adversary node attempts to perform communication in the network that results in establishment of wormhole tunnel between node S9 and node S2. Usually, such route establishment is done on minimal latency link to avoid getting caught. In such circumstances, when the mobile node S9 broadcasts its routing table than node S2 attempts to hear the broadcast using the wormhole tunnel and considers the wormhole tunnel as single hop channel. The routing tables are thereby adjusted by the neighbor nodes of S2 as well as the route via S2 in order to reach any of the mobile nodes S9, S10, S11, and S12. The problem becomes much worst as the adversary node can actually forward each bit over the wormhole tunnel directly even without waiting for an entire data packet to be received from S9. This exercise is performed to reduce the end-to-end delay invoked by the wormhole tunnel. Owing to the inherent invisible characteristics of attacker in the wireless mobile environment, the adversary node can generate a packet without addressing by itself as it can easily overhear them in the wireless transmission and directs (or tunnel) them to the colluding adversary at the other end of the tunnel (S2).

However, an interesting and unique point to be noted in this tunneling process is that if the adversary performs this routing honestly (for good purpose e.g. forwarding packet during congestion) than the network is not harmed or compromised. However, the tunnel could be misused by the attacker and could result in potential security damage. In such circumstances, it is not possible to mitigate any forms of attacks even of the communication is being performed with latest and sophisticated security protocols without any dependency of cryptographic key possession by the adversary. Another biggest issues is the invisibility of the adversary in the higher layers for which purpose the present security protocols are not able to identify the wormhole tunnel as well as the two colluding adversaries at the end point of the tunnel (as they are never visible).

3. NEED OF THE STUDY

Basically, even in presence of optimal security, if the invisibility characteristics of tunnel couldn't be solved till date, the problem to mitigate wormhole attack becomes more crucial. Particularly in MANET system, wormhole attack is quite impossible to detect as the nodes are in constant mobility owing to the dynamic topology. It is also known that AODV, DSDV, DSR, and OLSR are the most frequently used routing protocols in MANET. In case of DSR and AODV routing protocol, the adversary can perform the wormhole attack just by routing the RREQ control message directly to the destination target (S2). Upon hearing this RREQ message, the destination node performs re-broadcast the message and then decline the message without even processing all other received message (if the RREQ is forwarded from S9(regular node)). Wormhole attacks therefore resist any possible routes other than any routes through the tunnel. In case the adversary is in the proximity of the initiator of the route discovery process (could be any node), this attack can even resist routes more than two hops long from being discovered. It is to be noted that DSDV as well as OLSR also depends on the reception of the broadcasted packets as the medium for identifying their neighbor nodes and there are highly prone it attack. The discussion eventually means that usage of AODV, DSDV, OLSR, DSR are highly prone to wormhole attack. Therefore, the harmful effects of wormhole attacks are:

- Leads to corruption of routing information.
- Drastically degrade the data delivery process in large network.
- Also leads to other form of attacks e.g. black-hole attack, DoS, sinkhole attack, Sybil attack, etc.
- Allows adversary to gain illegitimate access, disrupt routing, and degrades network performance exponentially.
- Capable of launching cryptanalysis based attacks and can even crack keys.
- Can also lead to corruption of alarm or surveillance system.
- Services in physical layer are highly affected.
- Leads to permanent node partition problem in mobile adhoc network.
- Tunnel couldn't be traced by the existing IDS system and hence the original route information is damaged.

4. RECENT SURVEY STUDIES

This section discusses about the existing status of review work on various attacks in mobile adhoc network. For better information extraction, using various combination of search keyword 'wormhole attack', it was found that there are total of 220 Conference paper, 13 Journal papers, and only 2 Open Access papers in IEEE digital library with the year 2004-2014. Further, it was also found that there are many survey / review papers on the internet repositories, where wormhole attack was reviewed by many past authors with respect to Mobile Adhoc Network (MANET) as well as Wireless Sensor Network (WSN). Fig.2 and Fig.3 show the statistics of various types of survey papers on various attacks published in various international journals worldwide with respect to MANET and WSN. From the statistics exhibited in Fig.2, it can be seen that majority of the review papers have been published focusing on blackhole attack and then followed by wormhole attack in MANET. Whereas, as per statistics of Fig.3, survey papers related to wormhole attack in WSN are more in number. There are also survey work being done with the topic of common attacks like Sybil attack, cloning attack, and flooding (DoS) attack, rushing attack, sinkhole attack in both MANET and WSN. Hence, a common question may lie here that what is so significant in our present manuscript as it also deals with

review of wormhole attacks in MANET. The answer to this question may be replied with support of our findings depicted in Table 1 that shows the most recent survey papers on wormhole attacks in MANET. It is believed that the prime objective of the survey paper is to discuss the findings of the wormhole attacks and their prevention measures in such elaborate way that the findings will assist the future researcher to clearly understand the effectiveness as well as shortcomings of the techniques. Hence, keeping this motive, the investigation has been performed to find out that majority of the survey papers published till date are a kind of repetitive nature and hence more elaborate, impartial, and critical discussions are required. The research gap has been explored after reviewing various prior techniques discussed in Section VI.

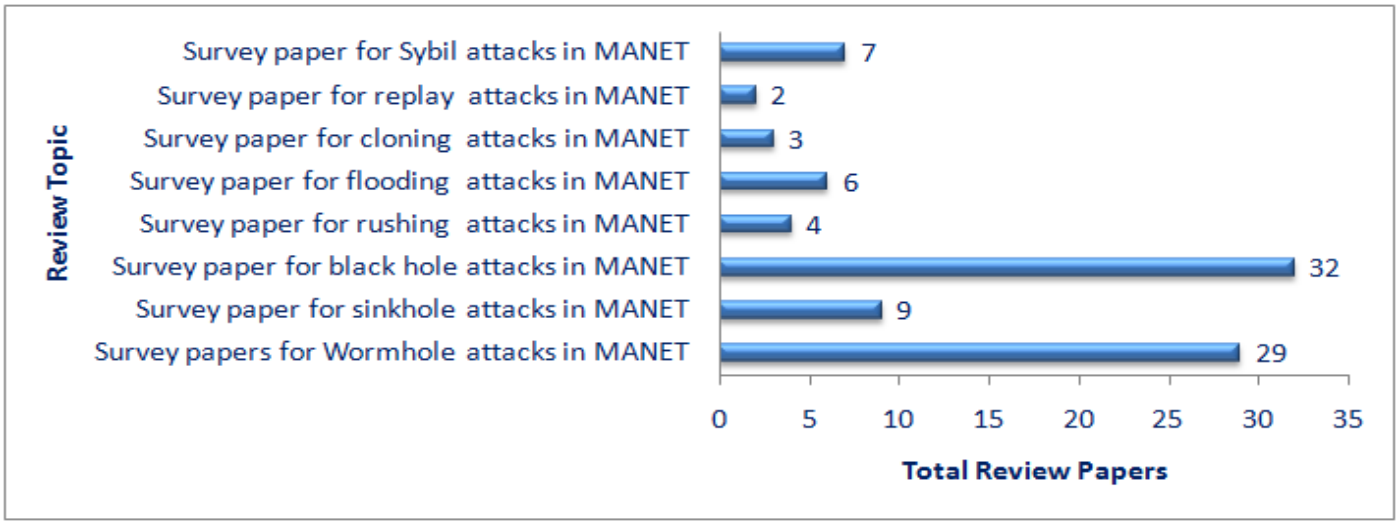

Fig 2: Statistics of Survey on various attacks in MANET (2004-2014)

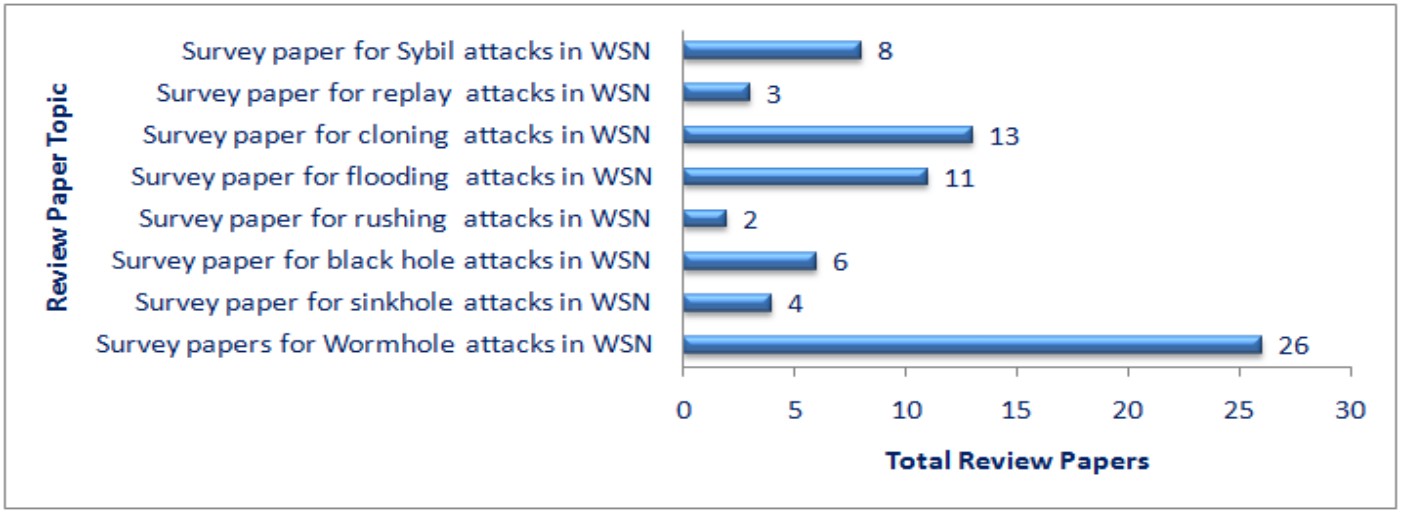

Fig 3: Statistics of Survey on various attacks in Wireless Sensor Network (2004-2014)

Table 1. Summary of Existing Survey Papers

Authors	Year	Topic in Focus	Inference
Maulik and Chakia [9]	2011	Routing Protocols, Wormhole attack classification, prevention techniques, metric to identify wormhole attack, Related work	Pros: Good Theory about the domain, studied comparison on the basis of synchronization, mobility factor, and quality factor. Cons: Very less description of techniques
Nigam et al. [10]	2011	Routing Protocols	Pros: Discussed theory on domain Cons: No discussion of prior implemented techniques at all. Title of paper doesn't match with the content of papers

Heidari [11]	2011	Prevention techniques and related work	Pros: Good discussion on prevention of wormhole attack approaches Cons: Extremely less narrowed discussion of prior techniques
Singh and Das [12]	2012	Brief discussion about IDS system in MANET, significant for wormhole attack, Related work discussion	Pros: Discussed 10 techniques theoretically for certain prior techniques Cons: Extremely narrowed discussion of prior techniques, prior outcomes not discussed explicitly
Kumar et al. [13]	2012	Impact of wormhole attack, prevention techniques, classification of wormhole attack,	Pros: Discussed comparison among 9 techniques Cons: comparison was studied on the basis of synchronization, mobility factor, and quality factor.
Arora and Goyal [14]	2012	Routing Protocols, attacks on MANET, wormhole attacks and their classification	Pros: Good Theory on routing protocol Cons: No discussion of prior implemented techniques at all
Garg and Sharma[15]	2012	Security issues in MANET, network security attacks, Byzantine wormhole attacks, related work	Pros: Good Theory on MANET Cons: Extremely narrowed discussion of 10 prior techniques
Dabas and Thakral [16]	2013	wormhole attacks and their classification, detection and prevention techniques	Pros: Good Theory on prevention techniques Cons: Extremely narrowed discussion of prior techniques. No explicit discussion towards understanding the effective contribution till date in the literature
Saluja & Gupta [17]	2014	Attacks on MANET, Wormhole attacks, related work	Pros: Good Theory on attacks in MANET Cons: Similar and repetitive technical discussion done by other survey papers
Patel & Patel [18]	2014	Attacks on MANET, Wormhole attacks, related work	Pros: Discussed 7 techniques of wormhole attack detection Cons: Extremely narrowed discussion of prior techniques
Kumai et al. [19]	2014	DSR, Wormhole attacks, related work	Pros: Discussed some techniques of wormhole attack detection Cons: No analysis of the contribution

5. EXISTING TECHNIQUES

There are various techniques that have been witnessed in the past for addressing the security issues arising from wormhole attacks in Mobile Adhoc Network. This section discusses explicitly those significant techniques in brief as follows:

5.1 RTT-based Techniques

In past, researchers have evolved up with a significant detection of wormhole attack based on round trip time (RTT). This is basically a time-bound approach where the time between senders's RTT and receiver receiving RTT information is estimated. The formulation is based on the theory that RTT of malicious neighbor nodes are quite high compared to regular nodes. This cost effective mechanism was pioneered by Gunther [20].

5.2 Temporal-Techniques

Wormhole attack could be identified using temporal approaches just like RTT based approach. The temporal factor determines the event of wormhole attack during route set up process by evaluating the transmission time between all the neighbor nodes lying on the signified path. The formulation is based on the similar fact of RTT based techniques, where the

temporal factor is found to be quite higher for malicious nodes compared to authenticated nodes. This approach was found to posses' better performance on overhead with no dependency on extra hardware. However, it was preliminary designed for AODV protocol. This approach was found to be introduced by Phuong et al. [21].

5.3 Statistical Approach

Statistical based approach is used for adopting probability theory in the process of identifying the wormhole attacks. As the malicious nodes are hard to find and eventually can exhibit confusing behaviour to avoid getting caught, hence statistical approach assist in mapping the routing behaviour and formulate strategies to detection and mitigate wormhole attack. Adoption of statistical approach was found in the work done by Upadhyay [22].

5.4 Packet Leashes

The term 'leash' can be defined as any additional information bound on the data packet for the purpose of safeguarding it to get compromised by wormhole attack. The prior studies have witnessed two types of packet leashing mechanism e.g. geographical and temporal packet leashes. The geographic packet leashing mechanism ensure the deterministic nature of the spatial distance between the sender and recipient while temporal approach ensure restriction to maximum travel distance based on time. However, such techniques require additional computation of time synchronicity. Evidence of this technique can be found in the work done by Hu et al. [23].

5.5 Digital Signature

Digital signature was found to be frequently used in cryptographic operations in MANET. However, this technique can also efficient mitigate wormhole attack in MANET. Usually such techniques calls for performing authentication using digital signature on the mobile nodes for sending the data packet, whereas on the other end, it performs validation of signature being generated. However, owing to adoption of sophisticated hashing function and decryption with public key, the signature generation as well as verification process is highly secured. Adoption of digital signature can be seen in the work done by Fatehpuria [24] and Akila et al. [25] most recently.

5.6 Digital Certificate

Usage of digital certificate is another frequently adopted technique for mitigating wormhole attacks in MANET. Usually in such technique, digital certificates are signed by private key of certificate authorities. Any other node with the authentic public key of the trusted CA can verify the certificate and thereafter use the public key of the node and be sufficiently sure that it indeed belongs to that node. Evidence of such technique can be found in work carried out by Dhillon et al. [26] and Anita et al. [27].

5.7 Fuzzy Logic based Approach

As the behavior of wormhole attack is a matter of uncertainty, where much vagueness prevails for identifying the location of compromised nodes. In terms of security technique, the behavior of the node is evaluated using trust factor that represents the level of reliability, where the trust level increases with increase of positive behavior of packet forwarding and on the other hand trust decreases with decrease if negative behavior (low packet forwarding). However, increased or decreased level of packet forwarding is the common feature for both malicious and regular node. Hence, such state of uncertainty is handled by fuzzy logic for assisting better computation of trust. Hence, under such circumstances, fuzzy logic was adopted by many researchers to mitigate such adversaries. Evidence of adoption of fuzzy logic can be found in the work carried out by Anusha [28], Manoj et al. [29], and Revathi et al. [30].

5.8 Cross-Layer based Approach

It is said that mobile adhoc network is highly vulnerable in its MAC layer where majority of the attacks targets to get launched. Hence, it is very important that node properties to be closely monitored from MAC layer to ensure better quality. Moreover, it is essentially important that routing and link layer be protected against any forms of breach in trust factor in MANET system. Hence, cross-layer approach comes as better alternative and was found to be adopted by various researchers e.g. Gopinath et al. [31], Raja ram [32], and Djahel et al. [33].

The other techniques found in the digital library are more or less combination or enhancement of the above mentioned techniques discussed by the researchers till date. Hence, it is very difficult to assess which one is the better version. Therefore, it has been classified based on two categories e.g. non-conventional and conventional publications. Non-conventional publications (Table 2) are those manuscripts with less impact factor and frequently in use by many researchers worldwide, especially in India. However, conventional publications (Table 3) are those, who have got superior standards like IEEE, Springer, Elsevier, ACM, Springer, InderScience etc.

Table 2. Techniques discussed in Non-conventional Journals

Authors	Techniques	Performance Parameters	Inference
Azer et al. [34]-2009-IJCSIS	Encapsulation techniques	-routes	😐 Outcomes are not benchmarked
Vijayalakshmi -[35]- 2011-IJCA	-Limiting Packet Propagation Parameter (LP^3) -Neighbor Aware Wormhole Adversary Axing($NAWA^2$)	No. of multicast group members	☺ Simple Design 😐 Outcomes are not benchmarked
Vani & Rao-[36]-2011-IJCSE	-Hop count based detection -Anomaly based detection -Wormhole isolation	Delay, Routing Overhead, Packet delivery ratio, Throughput	☺ Best suited for AODV 😐 Outcomes are not benchmarked

Haq et al.- [37]-2011-ICMLC	-Detection and Removal of colluding node	Time, packets	☹ Outcomes are not benchmarked, Not Scalable to larger network
Singh & Sharma-[38]- 2012-IRJES	-Intrusion Detection System	Positive predictive values, Negative predictive values, Specificity	☺ Higher applicability on VANET ☹ Outcomes are not benchmarked
Upadhyay- [39]-2012-IJCIS	-Statistical Analysis	-Load, Retransmission attempts, Throughput, Delay, Time	☺ Can locate malicious node ☹ Outcomes are not benchmarked, Not scalable in larger network
Jaiswal-[40] 2012-IJETT	Detection and prediction based scheme	-Not discussed	☹ Outcomes are not discussed
Niranjan et al.[41]- 2012-IJSR	Hop-count and delay based approach	-Average hop count & delay per route	☺ Reduces delay upto 75% ☹ Outcomes are not discussed efficiently and no potential bench-marking
Sebastian- [42]-2013-IJCNIS	Round Trip Time and Transitory Buffer	-Round Trip Time -Buffer	☺ Eliminate false positives in detecting wormhole ☹ Outcomes are not bench-marking
Shahnawaz -[43]-2013-IJET	Support Vector machine	-Trust, Accuracy, Precision Recall	☺ Benchmarked outcome shows 99% of accuracy. ☹ Use of SVM gives high algorithmic complexity and extensive memory requirements
Vandana-[44]-2013-IJSPTM	Multilayered Detection mechanism	Delay, Packet delivery ratio, Throughput	☺ Efficient compared to AODV ☹ Doesn't focus on packet modification behaviour of wormhole attack in MANET
Singh et al. [45]-2013-IOSR	Statistical Analysis	-false negative rate, control packet, energy	☺ lower false negative and controls energy drainage ☹ Justification of Algorithms are narrowed
Satheeshkumar [46]-2014-IJCSMA	Privacy protection	Packet delivery ratio, Latency	☹ No discussion of algorithm, outcomes, or benchmarking
Otmani-[47]-2014-IOSR	analyses the performance of AODV and DSR routing protocols with and without wormhole attack	Packet received, Throughout,	☹ So significant or breakthrough findings
Rafsanjani- [48]-Romanian Journal	SRP-Secured Routing Protocol using temporal leashes	Time of packet arrive	☹ No discussion of algorithm, outcomes, or benchmarking

Table 3. Techniques discussed in Conventional Journals

Authors	Techniques	Performance Parameters	Inference
Khalil et al.-[49]-2007-Elsevier	lightweight countermeasure for the wormhole attack-LITEWORP	% of malicious routes, % of true/false isolation, packet delivery ratio,	☺ Applicable to Sybil and sinkhole attacks too. ☹ QoS parameters not considered

Tran et al.-[50]-2007-IEEE	Transmission Time based Mechanism-TTM	-Transmission Time, False detection rate, Round Trip Time	☺ Applicable to other forms of attacks 😐 Experimented on smaller networks
Poovendran-[51]-2007 Springer	Graph Theory-spatial statistics theory	Radio patterns, length of link, guard densities, key	☺ Efficient technique 😐 outcomes not benchmarked
Vu et al. [52]-2008-Springer	Framework for defending against wormhole-WORMEROS	% of detection, false and true positive, Round trip time, delay	☺ Simple Technique 😐 outcomes not benchmarked
Khalil et al. [53]-2008- Elsevier	Mitigation of wormhole attack-MOBIWORP	Latency, drop ratio, % of isolation	☺ Ensure less memory overhead. 😐 study has not focused on preciseness and computational tractable way for gathering suspicion data
Khurana [54]-2008-IEEE	FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges	Overhead	😐 outcomes not benchmarked, length of the tunnel is not optimally used
Jen et al. [55]-2008-Sensors	Hop count analysis	Delay, false/true positives	☺ Effectively benchmarked with low overhead 😐 Doesn't focus on packet modification behaviour of wormhole attack in MANET
Li et al. [56]-2011-IEEE	Forced Collision on physical layer network coding	False positive alarm, bit error rate	☺ Less false positives 😐 outcomes not benchmarked
Gupta et al. [57]-2011-IEEE	Wormhole attack detection protocol using Hound Packet-WHOP	% of detection rate, no. of hound packet rate	☺ Effectively benchmarked with DELPHI protocol 😐 QoS factors not discussed, hound packet not optimized, processing delay not addressed effectively.
Stoleru et al. [58]-2012	Mobile Secure Neighbor Discovery	false/true positives, Ranging and Travel error	☺ performed real-time evaluation 😐 outcomes not benchmarked
Matam [59]-2013-EURASIP	Wormhole-resistant secure routing for wireless mesh networks-WRSR	Packet delivery ratio, Length of wormhole	☺ Benchmarked outcome with good packet deliver ratio 😐 QoS factors not benchmarked
Kim et al. [60]-2013-Hindawi	Transmission-Time based Wormhole detection	% of detection rate, time	☺ benchmarked outcome shows higher extent of detection rate 😐 False positive is not significantly improved with increase of time interval
Shi et al. [61]-2013-IEEE	Random delay multiple access (RDMA) protocol	Normalized number of time slots, rate of successful transmission nodes,	☺ effectively prevent and detect wormhole attack for 60 GHz network 😐 Less Effective Benchmarking

6. RESEARCH GAP

Following are the research gap after reviewing the papers included in the proposed survey:

6.1 Narrowed Survey

Table.1 has briefed all the existing review work that has been published during the year 2011 till date. It can be seen that majority of the review work done till date highlights the theoretical background of the nature of the wormhole

detection and prevention measures of repeated nature in almost all the existing review papers. The existing review papers are significantly missing better classification of the studies and discussion of the outcomes with respect to the performance parameters. Comparative analyses discussion with an aid of performance parameters of the existing studies are very much critical as it assist the reader to understand the most efficient technique till date. Majority of the contents of the existing review papers are repetitive in nature with other survey papers and no significant outcomes could be derived after gathering or reading the survey papers.

6.2 Few benchmarked Studies

From the information highlighted in Table 2 and Table 3, it can be seen that majority of the existing studies [34] [35] [36] [38] [39] [42] [48] etc are not benchmarked at all. Hence, it becomes really a challenging situation to understand the reliable nature of the discussed research papers. Benchmarking assist the readers as well as the authors to prove that under what circumstances their outcomes are superior to someone's work. If such critical information is missing from the existing implementation, adoptions of such work are less likely to happen for future researcher.

6.3 Repetitive Nature of Implementation:

The reason why it is chosen to segregate the papers with respect to publishers based on their impact factor, as because usually standard publishers like IEEE, Springer, Elsevier, etc are found to have better scrutinizing policies for the manuscript, which are not that much emphasized by other non-standard publishers. From the Table.1, it can be seen that some of the studies are just the remake of some research work discussed in Table 2. For an example, the work proposed by Vani and Rao [36] in 2011 has adopted hop count based detection, anomaly based detection, and wormhole isolation, which is almost similar to the work done by Jen et al. [55] in 2008. The statistical analysis as a method to detect wormhole attack is found to be adopted by Upadhyay [22] in 2012 and the similar technique was also found to be adopted by Singh et al. [45] in 2013. Adoption of Round Trip Time as technique to identify the compromised routes was witnessed in the study of Sebastian [42] in 2013, which was originally adopted by Tran et al. [50] in 2007. Hence, very few novel and unique approaches are found in literature.

6.4 Less Effective Performance Parameters

It is strongly believed that selection of performance parameter play a strong role for ensuring the detection of wormhole attack. It can be seen from Table 2 and Table 3, that majority of the authors have selected percentage of detection rate as the core performance parameter, which are eventually checked from true or false positive. Well, the above mentioned researchers are right in their techniques but selecting percentage of detection rate only helps to identify the success factor in detection operation of the presented techniques of past. However, various questions arises that i) what is the issues of wormhole attack on energy of nodes? (as mobile nodes constantly depletes their energy during mobility), ii) is there any predictive parameter to identify the unstabilized links before establishing routing? iii) What extent the compromised node affects the control message dissemination after the attack? and many more. Such questions were never solved or addressed in past. It was also seen that adoption of Quality of Service (QoS) parameters e.g. energy, bandwidth, jitter, latency etc are very much less explored as the possibility of considering as an effective performance parameters.

7. CONCLUSION

Owing to the dynamic topology in mobile adhoc network, the MANET system is already encountering various issues pertaining to energy, routing, quality of services etc. However, security problems have become more critical and are also closely link with the all the problems associated with its inherent characteristics of dynamic topology and decentralized nature. This paper has studied around 61 cited research paper and 235 uncited researches paper, and came to four concluding points:

- The first conclusion is that survey papers published till date doesn't provide significant information about the effectiveness of the prior mitigation techniques of wormhole attacks. The existing survey papers are highly theoretical and posses few extent of descriptive highlights on the past techniques.
- The second conclusion of the study is that there are massive volumes of research manuscript being published till which are categorized in conventional and non-conventional international journals. The findings suggest that 50% of the work (focusing on mitigation of wormhole attacks in MANET) published till date in non-conventional journals are inspired (or enhanced) from conventional journals. Hence, the extent of novelty in the mitigation techniques are quite less inspite of more number of research papers availability.
- The third concluding point is every techniques discussed on conventional research manuscript have some prominent advantages and as well limitations. Hence, a suggestion has been given that inspite of designing any intrusion detection or prevention system for wormhole attack in MANET, it is important that emphasized could be laid on malicious behaviour of wormhole and tunneling process. This is very critical to consider as slight loophole in any mitigation technique could result in inviting other attack forms (like Sybil attack, blackhole attack, sinkhole attack etc).
- The fourth concluding point is that there is lesser extent of studies being focused using mathematical approaches. Majority of the study adopts cryptographic technique, time-based techniques, digital signature, or fuzzy logic. Hence, it is suggested that future researcher should also investigate more behavioral-based technique to understand the malicious behaviour of wormhole attacker so that effective mathematical modelling can be performed.

Hence, in a nutshell, it can be said that technique for mitigating wormhole attack are still in infancy stage and much effectiveness as well as novelty in wormhole attack modelling techniques are not yet introduced till date. Extensive investigation about the security algorithm is higher required that can model the malicious behaviour of wormhole attack in MANET. Hence, our future direction of the study will consider all these attribute and focus on i) effective mathematical modelling of wormhole attack ii) ensuring computational effectiveness of mitigation technique, iii) performing benchmarking of the future technique with extended performance parameters to ensure scalability and efficiency of our future work.

8. REFERENCES

[1] Basagni, S. , Conti, M., Giordano, S., Stojmenovic, I.2013. Mobile Ad Hoc Networking: The Cutting Edge Directions. John Wiley & Sons. Technology & Engineering.pp. 888

[2] Boukerche, A.2005. Handbook of Algorithms for Wireless Networking and Mobile Computing. CRC Press, Computers. pp.1040

[3] Priyanshu and Maurya, A. K.2014. Survey: comparison estimation of various Routing protocols in mobile ad-hoc Network. International Journal of Distributed and Parallel Systems. Vol.5, No.1/2/3

[4] Udhayakumar, K., Prasanna, T., Venkatesan, Ramkumar, R.2014. Security "Attacks and Detection Techniques for MANET. Discovery. Vol. 15. No. 42

[5] Saha, H.N., Bhattacharyya, D., Banerjee, B., Mukherjee, S., Singh, R., Ghosh, D.2013. A review on attacks and secure routing protocols in MANET. International Journal of Innovative Research and Review, Vol. 1, pp.12-36

[6] Mamatha, G.S., Sharma, S.C.2010. Network Layer Attacks and Defense Mechanisms in MANETS- A Survey. International Journal of Computer Applications. Vol.9, No.9

[7] Zhang, Y., Zheng, J., Ma, M.2008. Handbook of Research on Wireless Security. Idea Group Inc (IGI), Computers, pp. 860

[8] Issac, B., Israr, N.2014. Case Studies in Secure Computing: Achievements and Trends. CRC Press, Computers, pp. 500

[9] Maulik, R., Chaki, N.2011. A study on wormhole attacks in MANET. International Journal of Computer Information Systems and Industrial Management Applications, pp. 2150-7988

[10] Nigam, N., Saraf, A., Nagar, C.2011. A Review New Thread Based Wormhole Attack Prevention Mechanism in MANET. International Journal of Electrical, Electronics & Computer Engineering, Vol.1 (1), pp. 84-87

[11] Heidari, A., Azad, I.2011. A Survey of Wormhole Attack and Countermeasures against that in Wireless Ad-hoc Networks. 5th Symposium on Advance in Science & Technology

[12] Singh, M and Das, R.2014. A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network. International Journal of Scientific & Engineering Research

[13] Kumar, S., Pahal , V., Garg, S.2012. Wormhole attack in Mobile Ad Hoc Networks: A Review. IRACST – Engineering Science and Technology: An International Journal, Vol.2, No. 2

[14] Arora, D., Goyal, S.2012. A Survey of Routing Protocols and Wormhole Attack in Mobile Ad Hoc Networks. International Journal of Research in Engineering and Applied Sciences. Vol. 2, Issue.2

[15] Garg, A., Sharma, S.2014. A Study on Wormhole Attack in MANET. International Journal of Scientific Research Engineering & Technology, Vol. 3 Issue. 2

[16] Dabas, P., Thakral, P.2013. Detection and Prevention of Wormhole Attack in MANET: A Review. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 3, Issue.3

[17] Saluja, B. K., Gupta, A.K.2014. A Survey of Different Approaches to Detect Wormhole attack.International Journal of Computer Science and I1nformation Technologies, Vol. 5 (3)

[18] Patel, B. N., Patel, T.S.2014. A Survey on Detecting Wormhole Attack in Manet. Journal of Engineering Research and Applications, Vol. 4, Issue. 3, pp. 653-656

[19] Kumari, H., Vyas, G., Dhankar, S.2014. A Survey of Wormhole Detection and Prevention Technique in DSR Protocol. International Journal of Engineering, Management & Sciences, ISSN: 2348 –3733, Vol. 1, Issue. 9

[20] André, G., Hoene, C. 2005. Measuring round trip times to determine the distance between WLAN nodes., Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks, Mobile and Wireless Communications Systems, pp. 768-779

[21] Phuong, T.V., Canh, N.T., Lee, Y-K., Lee, S.,. Lee, H.2007. Transmission time-based mechanism to detect wormhole attacks. IEEE Asia-Pacific Service Computing Conference, pp. 172-178

[22] Upadhyay, S., Bajpai, A.2012. Avoiding Wormhole Attack in MANET using Statistical Analysis Approach. International Journal on Cryptography and Information Security, Vol.2, No.1

[23] Y.-C, Hu., Perrig, A., Johnson, D.B.2003.Packet leashes: a defense against wormhole attacks in wireless networks. INFOCOM

[24] Fatehpuria, A. K., Raghuwanshi, S.2013. An Efficient Wormhole Prevention in MANET through Digital Signature. International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue.3

[25] Akila, T., Uma Maheswari, P., Sivanandam, S.N.2014. TQDS: Time Stamped Quantum Digital Signature to Defend Wormhole Attack in Wireless Sensor Network. International Journal of Research in Engineering and Technology, Vol. 03, Issue. 07

[26] Dhillon, D., Randhawa, T. S., Wang, M., Lamont, L.2004. Implementing a fully distributed certificate authority in an OLSR MANET. In Wireless Communications and Networking Conference, Vol. 2, pp. 682-688

[27] Anita., Mary, EA., Vasudevan, V., Ashwini, A.2010. A certificate-based scheme to defend against worm hole attacks in multicast routing protocols for MANETs. IEEE International Conference on Communication Control and Computing Technologies Conference , pp. 407-412

[28] Anusha , K., Jayaleshwari , N., Kumar, A., Rajyalakshmi, G.V.2013. An Efficient And Secure Intrusion Detection Method In Mobile Adhoc Network Using Intuitionist Fuzzy, International Journal of Engineering and Technology, Vol 5 No. 3,

[29] Manoj, V., Aaqib, M., Raghavendiran , N., Vijayan, R.2012. A Novel Security Framework using Trust and Fuzzy Logic in Manet. International Journal of Distributed and Parallel Systems, Vol.3, No.1

[30] Revathi, P., Sahana , M. M., Dharmar, V.2013. Cross Layer Detection of Wormhole In MANET Using FIS. ITSI Transactions on Electrical and Electronics Engineering, Vol. 1, Issue. 3

[31] Gopinath, S., Nirmala, S., Sureshkuma, N.2012. Misbehavior Detection: A New Approach for MANET. International Journal of Engineering Research and Applications, Vol. 2, Issue. 1, pp. 993-997

[32] Rajaram, A., Palaniswami, S.2009. A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks. International Journal of Computer Science and Information Security. Vol. 6, No. 1

[33] Soufiene,D., N-Abdesselam, F., Khokhar, A.2009. A cross layer framework to mitigate a joint MAC and routing attack in multihop wireless networks. IEEE Conference on Local Computer Networks, pp. 730-737

[34] Azer, M., E-Kassas, S., E-Soudani, M.2009. Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks.International Journal of Computer Science and Information Security, Vol. 1, No. 1

[35] Vijayalakshmi, S., Albert Rabara, S.2011. Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP^3 and NAWA. International Journal of Computer Applications, pp. 0975 – 8887, Vol.16, No.7

[36] Vani, A., Rao, S. 2011. A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks. International Journal on Computer Science and Engineering, Vol. 3, No. 6, 2011

[37] Haq, S. U., Hussain and, F. B., Hassan, H. M.2011. Out-of-band Wormhole Attack Detection in MANETs. 3rd International Conference on Machine Learning and Computing, 2011

[38] Singh, J. , Sharma, N. 2012.An Advanced IDS Approach to Detect Wormhole Attack in VANET. International Refereed Journal of Engineering and Science, Vol.1, Issue. Vol.3, pp. 09-12

[39] Upadhyay, S., Bajpai, A.2012. Avoiding Wormhole Attack in MANET using Statistical Analysis Approach. International Journal on Cryptography and Information Security, Vol.2, No.1

[40] Jaiswal, S., Agrawal, S.2012. A Novel Paradigm: Detection& Prevention of Wormhole Attack in Mobile Ad Hoc Networks. International Journal of Engineering Trends and Technology. Vol.3, Issue.5

[41] Niranjan, P., Srivastava, P., Soni, R.K., Pratap, R.2012. Detection of Wormhole Attack using Hop-count and Time delay Analysis. International Journal of Scientific and Research Publications, Vol. 2, Issue. 4

[42] Sebastian, M., Kumar, A.R.2013. A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer. Computer Network and Information Security, Vol. 8, pp. 28-38

[43] Shahnawaz, H., Joshi, R.C., Gupta, S.C.2013. Design of Detection Engine for Wormhole Attack in Adhoc Network Environment. International Journal of Engineering and Technology, Vol. 4, No 6

[44] Vandana, C.P., Devaraj A. F. S.2013. MLDW- a Multilayered Detection mechanism for Wormhole attack in AODV based MANET. International Journal of Security, Privacy and Trust Management, Vol. 2, No 3

[45] Singh, P., Srivastava, A., Gupta, N. 2013. A Novel Approach to Detect & Prevent Wormhole Attack over MANET & Sensor n/w towards Lower Battery Power Consumption. Journal of Computer Engineering, Vol. 15, Issue. 1, PP 51-58

[46] Satheeshkumar , B., Kalaivani, R. 2014.Privacy Protection against Wormhole Attacks in Manet. International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, pp. 56-62

[47] Otmani, M., Ezzati, A.2014. Effects of Wormhole Attack On AODV and DSR Routing Protocol Through The Using NS2 Simulator.Journal of Computer Engineering, Vol.16, Issue. 2, pp. 1 01-107

[48] Rafsanjani, M.K.,.Samani, M.E.2013. Resist SRP against Wormhole Attack. Romanian Journal of Mathematics and Computer Science. Vol. 3, Issue. 1, pp.60-70, 2013

[49] Khalil, I., Bagchi, S., Shroff, N. B.2007. LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks. Computer networks, Vol.51, No. 13, pp. 3750-3772

[50] Tran, P.V., Lee, Y-K., Hung, L. X., Lee, S., Lee, H.2007. TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks. In Consumer Communications and Networking Conference, pp. 593-598

[51] Poovendran , R., Lazos, L.2007. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks, Vol. 13, No. 1, pp. 27-59

[52] Vu, H., Kulkarni, A., Sarac, K., Mittal, N.2008. WORMEROS: A New Framework for Defending against Wormhole Attacks onWireless Ad Hoc Networks. Springer-Verlag Berlin Heidelberg

[53] Khalil, I., Bagchi, S., Shroff, N. B.2008. MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks", Ad Hoc Networks, Vol. 6, No. 3, pp. 344-362

[54] Khurana, S., Gupta, N.2008. FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks. In Emerging Security Information, Systems and Technologies, Second International Conference, pp. 74-79

[55] Jen, S-M., Laih, C-S., Kuo, W-C.2009. A hop-count analysis scheme for avoiding wormhole attacks in MANET. Sensors, Vol. 9, No. 6, pp. 5022-5039

[56] Li, Z., Pu, D., Wang, W., Wyglinski, A.2011. Forced collision: detecting wormhole attacks with physical layer network coding.Tsinghua Science & Technology, Vol. 16, No. 5,pp. 505-519

[57] Gupta, S., Kar, S., Dharmaraja, S.2011. WHOP: Wormhole attack detection protocol using hound packet. International Conference In Innovations in Information Technology , pp. 226-231

[58] Stoleru, R., Wu, H., Chenji, H.2012. Secure neighbor discovery and wormhole localization in mobile ad hoc networks. Ad Hoc Networks, Vol. 10, No. 7, pp. 1179-1190

[59] Matam, R., Tripathy, S.2013. WRSR: wormhole-resistant secure routing for wireless mesh networks, Journal on Wireless Communications and Networking, Vol.180

[60] Kim, D-K., Kim, H-W., Kim and, G., Kim, S.2013.Research Article a Counterattack-Detection Scheme in Transmission Time-Based Wormhole Detection Methods. International Journal of Distributed Sensor Networks, pp. 6

[61] Shi, Z., Sun, R., Lu R., Qiao, J., Chen, J., Shen, X. U. E. M. I. N.2013. A Wormhole Attack Resistant Neighbor Discovery Scheme With RDMA Protocol for 60 GHz Directional Network. Emerging Topics in Computing