International Journal of u- and e- Service, Science and Technology
Vol.10, No.12 (2017), pp.13-22
http://dx.doi.org/10.14257/ijunesst.2017.10.12.02

Comparative Analysis of Various Techniques for Detection and Mitigation of Wormhole Attack in MANET

Gulshan Kumar[1], Manpreet Kaur[2], Mritunjay Kumar Rai[3], Rahul Saha[4*], Hye-jin Kim[5] and Rajeev Kandey[6]

[1,2,4,6]Department of Computer Science and Engineering, Lovely Professional University
[3]Department of Electronics and Communication Engineering, Lovely Professional University
[5]Business Administration Research Institute, Sungshin W. University, Seoul, Republic of Korea
**rsahaaot@gmail.com*

Abstract

In this paper we study different approaches regarding MANET security attacks at network layer and compare for their functionality and procedure. Some approaches based on the detection and prevention schemes and other for correction of those attacks. In our study, we compare the different aspects of security attacks detection and prevention. Each with different advantages and disadvantages. The main focus will be on wormhole attack detecting, preventing and mitigating schemes. In this paper, we will compare approach for solving the issues among discussed papers. The comparison table is prepared for summarizing the conclusions.

Keywords: *MANET, Security attacks, Wormhole attack*

1. Introduction

MANET is growing very fast and trending these days. Many researches has been already done, but still there are many areas to explore. One problem can be seen in different aspects and can be solved by different solutions. MANET is very prone to security threats due to its openness, adaptability, infrastructure properties, decentralization and self-organization. Hence, security becomes an important aspect to look at in MANET. There are different types of attack[1] present at network layer. Some are described as follows:

- **Wormhole**[2][19][20]**:** In this attack, two or more malicious nodes try to form a tunnel by using high speed network devices or cables. These nodes capture packet at one end and send it at another end and broadcasts it there. These nodes announce themselves having shortest path to the destination. So, other nodes always choose these nodes for routing packets, leading to failure of packet delivery to intended destination.
- **Black hole**[3]**:** In this attack, malicious nodes announce that they have valid and shortest path to destination. But in actual they have not, sequentially other nodes choose these nodes as routing path. When nodes send packet through it, then malicious nodes will drop all the packets that it captures. Hence, data packets lost.

Received (September 3, 2017), Review Result (November 6, 2017), Accepted (December 5, 2017)
* Corresponding Author

ISSN: 2005-4246 IJUNESST

- **Gray hole**[4]**:** In this attack, malicious nodes form blackhole, but it only drops the packets for some particular nodes and for some particular time. It is different to detect than blackhole attack, as only for some nodes it behaves maliciously while for others it is a normal node.
- **Denial of service**[5]**:** In this attack, malicious node send flood of data packets to victim, so as to block it from providing any services to other nodes. Mostly the victims are high speed end servers. Malicious nodes send huge chunks of data to these servers continuously to make servers busy processing its requests and not processing other valid requests coming from valid nodes.
- **Vampire Attack**[6]**:** In this attack, malicious node send data packets to victim node to increase the power consumption and resource usage of victim node. The data packets send by malicious nodes consumes most of the power of the victim nodes and drain victim nodes power. Malicious nodes are also called vampire nodes. This attack is difficult to detect as it does not modify or alter any data packets but passively draining energy resources for a particular victim node.
- **Byzantine Attack**[7]**:** In this attack, malicious intermediate nodes or group of malicious intermediate nodes gives false routing information and creates routing loops also forward data packets to non-optimal path which may be harmful to routing system.

In this paper, we study different papers. Each one is describing the problem i.e. security attacks like wormhole, black-hole, etc. and providing with a solution for the same. We are now comparing their work for better aspects.

2. Literature Review

In order to come to a conclusion, we first need to gather knowledge of that particular topic. In this study, we also review available literature on wireless sensor networks and wormhole attack which describes the state of art of the topic very well. In our literature review we found different techniques in order to mitigate the problem. But they are not enough for the growing need of security for the networks.

In study of **detection and prevention of wormhole attack in wireless sensor networks using AOMDV protocol**[8] proposed by **Parmar Amish and V.B. Vaghela**., aims to detect and prevent wormhole attack in WSN using AOMDV protocol. According to the proposed work, when source node broadcasts RREQ packet, it will note the time, t. Then for each RREP received by source node, time is noted, say, tr. Sender node then calculates round trip time for all routes using formula, tx=tr-t. Then threshold round trip time is calculated by using formula, z= tx1+tx2+txi/i. if tr is less than threshold and hop-count on route i is equals to 2 the it detects that route i as wormhole link. Ender detects first neighbour node as wormhole node. Then sender sends dummy RREQ through route i. receiver on receiving dummy RREQ from its neighbour and detects it as wormhole node. Routing entries for that route is removed from routing table and broadcasts to other nodes as well. The parameters for performance measurements are throughput, delay and packet delivery fraction. No special hardware is required. It performs well in dense networks. Less end to end delay and improved packet delivery fraction. But mobility mode is fixed also overhead in calculating round trip time for every node.

In study of **design and implementation of trust based approach to mitigate various attacks in mobile ad-hoc networks**[9] presented by **Nilesh N. Dangare and M.S. Mangrulkar**, the aim is to mitigate Vampire and DDoS attacks. They proposed a technique in which they form a cluster based network, then selection of two nodes having highest energy called trusted nodes, takes place. Then packets and route responses for each node in network is counted. After this a comparison of threshold value with counted values has been made to get malicious nodes. Lastly routing table of nodes are updated

accordingly. They choose AODV routing protocol as it is loop free and no central administration is required also it avoids count to infinity problem. This technique use no special hardware. Overhead of calculations is also less and it is easy to implement. But it restricts its functionality to very low mobility networks. It fails when network is highly dynamic and continuously changing.

In study of **wormhole free routing and DoS attack defence in wireless mesh networks**[10] presented by **G. Akilarasu, S. Mercy Shalinie**, aims to introduce technique that find wormhole free routes in networks by some finite state model and priority mechanism. The authors apply finite state model in which node keeps info of sender and receiver with neighbour nodes. Each node acts as monitor node, each monitor checks sequence of local message block with authorized certificates. For some T seconds, it runs detection algorithm which classifies them in- selfish nodes and cooperative nodes. By collecting information from RREQ and RREP, wormhole links are detected and then wormhole aware routing is initialized. Then routes free from wormhole is selected. For detecting DoS attack a priority table is created for each node. Packets with low priority is discarded first to ensure transmission of legitimate nodes. Then corresponding DoS attackers are removed from the network by edge routers. The parameters for performance measurement are packet delivery ratio, packet drop and delay. It requires no special hardware. Wormhole free routes are discovered. No additional information regarding location is needed. Lesser delay than WRSR. Less packet drop than WRSR. Delivery ration is also more in case of WRDAD. Eliminates both selfish and DoS attacker nodes. It induces overhead, also not efficient for dynamic topology. Length of wormhole may affect the discovery of wormhole routes. Based on the finite state model and priority mechanism malicious nodes in network is easily discovered and selfish or DoS node are removed from the network. This scheme is also reducing packet drop and increases packet delivery ratio. Future scope can be presented in dynamic network.

In study of **WRSR**, that is, **wormhole resistant secure routing for wireless mesh networks**[11] proposed by **Rakesh Matam and Somnath Tripathy**, aims to detect presence of wormholes during route discovery process. In this proposed work authors allow nodes to monitor two-hop sub-path on received RREQ and identify RREQ that traverse wormhole. Nodes maintain neighbourhood relations with all nodes in their two-hop range. For this extended Ethernet beacon frame including flag bit and neighbour address is used. Route discovery is similar to HWMP but additional verification for RREQ is applied, intermediate nodes received broadcasted RREQ and verifies their identity for two-hop neighbours and sub sequentially create routing entry for corresponding RREQ_ID, sets its state as transient and rebroadcasts it. Otherwise drops it. Then wormhole free paths are selected for routing. The parameter used to measure the effectiveness are detection rate, false positives, impact of wormhole and impact of node degree. The proposed work is able to defend against all types of wormholes with no extra requirement of specialized hardware. No synchronized clocks and no cryptographic mechanisms are required. But If no alternate path discovered in case if present path is leading to wormhole, then node need to re-initiate route discovery, all process need to be re-done. It fails to detect wormhole link when both wormhole nodes are neighbour of each other. We learnt that proposed protocol relies on shorter alternate paths to detect wormhole link and discover wormholes during route discovery process. The probability of finding alternate paths free from wormhole link has been computed and shown highly in uniformly distributed networks.

In study of **comparative study on wormhole attack prevention schemes in MANET**[12] presented by **Subhashis Banerjee and Koushik Mujumdar**, aims to carry out detailed comparative analysis of well-known countermeasures against wormhole attack according to their relative advantages and disadvantages. The authors compare different protocols such as, wormhole attack on periodic protocols, wormhole on on-demand protocols, wormhole attack against local broadcast protocols. Then review of

countermeasures against wormhole attack is done by taking protocols under consideration such as, location based and time based protocols, end-to-end detection of wormhole attack protocols, hop-count analysis based schemes, statistics based solutions. Lastly comparison between these countermeasures are performed. The different parameters for comparison is packet travelling time, detection stage, detection rate, specialized hardware required, computation overhead, delay, radio propagation model, detection of closed wormholes available, storage overhead, communication overhead, cryptographic mechanisms required, power efficiency, byte overhead and message overhead. This work exploit the features of different types of protocols and helps to find out efficiency of proposed protocols. Different parameters are used to measure their performance effectiveness. It also provides the basic information about wormhole attacks. Protocols suffer from their own weaknesses. Need specialized hardware required. Larger overheads due to computation, communication, message, packet size and storage capacity. Most protocols proposed are not sufficient for MANET. Routing protocols for MANET are vulnerable to inherent design disadvantages. There is still huge scope of research in field of wormhole detection and prevention. Most of the proposed mechanisms suffer from their own weaknesses Proposed methods are not sufficient to detect wormhole attack completely. Time synchronization based prevents only closed wormhole attack. Statistical analysis based prevents multiple wormholes but require enough routing information and low mobility network. Reliability of hop count based are inversely proportional to communication overhead. A technique is required which combine features of both software and hardware driven techniques.

In study of **secure routing in mobile wireless ad hoc networks**[13] presented by **Siddhartha Gupte, Mukesh Singhal**, aims to criticize and get to know available protocols aimed at secure routing in mobile wireless ad hoc networks. In this piece of work, at very first, possible attacks on routing protocols are categorized and explained differently and very unambiguously. After that properties that should be in a secure routing protocol is discussed. Then some protocols such as security aware ad hoc routing protocol, ARAN protocol, ARIADNE, TESLA, on demand secure routing protocol, SEAD etc. are explained very precisely with this, self-securing ad hoc wireless networks, mitigating malicious behaviour and optimized inter-router authentication scheme is discussed. The parameters to measure the effectiveness are number of packet dropped, throughput, delay and number of false positives. Every protocol has different advantages and disadvantages. Further work can still be done in given areas. No protocol is in all aspects is efficient for routing and we cannot say all present protocol are fail-safe or secure. Future research can be done in securing routing in networks.

In study of **countermeasures against wormhole attacks in MANETs using analytical hierarchy process methodology**[14] proposed by **Fei Shi, Weijie Liu, Dongxu Jin and Jooseok Song**, aims to elect local most trustable nodes for source and destination to detect and locate wormholes using analytical hierarchy process. The authors proposed electing LMT nodes with largest weight value for source and destination by using relative stability of node, credit value of node and reciprocal of forward rate of node. AHP is measurement of pairwise comparisons and priority scales to elect LMT nodes. To elect LMT first define problem then structure design hierarchy afterwards construct set of pairwise comparison matrices lastly compute weights and use priority scales to elect LMT node. Then LMT node will perform countermeasure against wormhole. First is detecting phase, in which LMT node will set timer for HELLO messages sent and HELLO reply received. Then minimum hop is estimated proceeding with hop count extracted from RREP. After this locating phase started, LMT node set its timer for TRACE sent and TRACE reply received. Then Hop count is tested by comparing current value with last obtained values by which location of wormhole is located. At last bi-directional location mechanism phase starts, to solve collaborative wormhole issue. First timer is set by LMT node for TRACE sent and TRACE received

after this hop count is tested with previous count received, if no wormhole is identified then LMT node of source store intermediate node's RTT info then it sends this info to destination LMT node via secure path. Then TRACE is sent by destination LMT node in inverse direction of same path, timers are set, intermediate node replies TRACE reply to destination LMT node. Then destination LMT nodes will specify wormhole nodes by checking hop count comparison. If wormhole still could be identified, then previous step repeated again to identify and locate collaborative wormhole node. The parameters used to measure effectiveness are number of false positives, number of wormhole located, number of invalid links removed and number of valid links removed. It can detect as well as locate wormhole nodes. It is a hierarchical approach and use bi-directional location mechanism which might pin point the exact location of wormhole node. It elect LMT nodes for more security of packet transmission. No special hardware is required. Every node has uniform security level. It has large computation overhead. If wormhole not identified in one step, then again that step is iterated number of times. The assumed network is Static. Computations are time consuming. It is also difficult to implement in dynamic and continuously changing environment. Wastage of resources if wormhole does exist in network. Delay in transmission of packets with bulk of computations performed. Scheme has overhead in calculating weight values also delayed transmission. When node moves to new neighbourhood it becomes stranger to its neighbour. More parameters can also be used for calculating weight values. Proposed scheme can be extended for other MANET security attacks like blackhole attack. In future, simulation can be done in NS2 with two scenarios with and without wormhole attacks, if first we calculate network throughput and in latter we will measure delivery rate enhancements due to our proposed scheme.

In study of **secure neighbourhood creation in wireless ad hoc networks using hop count discrepancies**[15] proposed by **Thaier Hayajneh, Prashant Krishnamurthy, David Tripper and Anh Le**, aims to create secure neighbourhood by using hop count discrepancies in routing to detect true neighbours and remove those links that appear to be neighbour but in real are not. In the proposed work by authors, source node will discover its one-hop neighbour by sending "hello" message. Cryptographic techniques used to prevent malicious nodes from sending fake replies. Neighbours could be elements of either NA or NA*, source cannot distinguish between these sets. Source wants to determine if b is true neighbour then source asks b to provide its one-hop neighbour list NB. Source picks some nodes belongs to NB-NA and makes it as target node T. Source will ask its neighbour to find shortest paths to T, paths must not be direct and avoid one0hop neighbours NA and NB of both source and B. Source node employs select(route) and compare with route that pass-through wormhole, which should be 3-hops. If difference between selected route and wormhole route is > threshold n then SECUND declares wormhole in vicinity, n must be a smaller value. Detection process is improved by using mutual detection. Wormhole will be suspected iff both A and B discover their links connected through wormhole. If source node asks its neighbour that are not part of NB to find routes to neighbour NB that are not part of NA, if routes found are long then process stops. Then b is flagged and link is removed. The parameters used to measure effectiveness are false positives without mutual checks, percentage of legal links removed by mistake, percentage of false positives with mutual checks, removal of bogus and legal links, impact of wormhole length, impact of node degree and overhead analysis. There is small overhead in terms of number of links checked for wormholes. No special hardware requirements. No need for location information. No need for very high node degree. No need for accurate synchronization between nodes. But it does not work well with high value of n. If critical node exists in network, it fails. It fails when source picks bogus node as target node. It has not defined protocol suitability for removal() algorithm for removal of bogus links. SECUND employs co-operation between neighbouring nodes for creating secure neighbourhood by using routing hop discrepancies between neighbours to

determine existences of wormhole and remove bogus links created by wormholes. SECUND is simulated over different distributions of nodes in network and different types and length of wormholes. It demonstrated excellent wormhole detection rate with few false alarms, also capable of removing bogus links from network while removing only few legal links if any.

In study of **localized wormhole detection and prevention in wireless networks**[16] presented by **Tassos Dimitriou and Athanassios Giannetsos**, aims to defend against wormhole attacks in wireless networks by not adopting any synchronized clocks, positioning devices or directional antennas. This work is based on assumptions:

1 SMA1: all sensor nodes run some neighbour discovery routine and can record their neighbour ids.

2 AMA1: wormhole link is long enough so that regions A and B are well separated from each other

3 AMA2: there is some initial interval t where no attack is taking place and nodes can safely establish neighbourhood information.

Wormhole detection and prevention look for simple path between two nodes that indicates absence of wormhole link between them. Algorithm is strictly localized and only nodes undergo topology changes need to run it. Each node u, upon discovery of new suspect node v, searches for such paths using k-hop neighbourhood knowledge. K should be a small value. The parameters for the performance measurements are finding small paths between pair of nodes, path existence percentage, detection time, memory footprint and time required for each set of wormhole detection and prevention. It only uses connectivity information. No specialized hardware. It will always prevent wormholes. It is efficient in memory requirement and processing overhead and also it is fails safe, easy to implement and suits well for dynamic networks. But attacker can fool algorithm by using small wormholes. It Fails if attacker make fake links in neighbourhood of wormhole end-points. It is also unable to prevent combined wormhole attack. It is investigated that Wormhole detection and prevention always prevent wormhole attacks, it allows legitimate node to addition with high probability, even for low density networks. It is lightweight enough to run on sensor nodes. This algorithm has practical use in real-world scenarios and can be considered as reference point for future investigations of more attractive solutions against wormhole attacks.

In study of **local connectivity tests to identify wormholes in wireless networks**[17] proposed by **Xiaomeng Ban, Rik Sarkar, Jie Gao**, aims to detect and remove wormhole using local connectivity tests. This approach is to examine graph connectivity and detect fundamental connectivity change. This approach is classified into four steps:

- rigorous definition of wormhole attack.
- guaranteed detection on wormhole sets
- robustness to different communication models and dimensions
- scalability and communication costs

The parameters used to measure effectiveness are effect of sensitivity, influence of size of neighbourhood to be removed and elimination of false alarms. It guarantees to detect true wormhole nodes. Longer wormholes are easy to detect. Wireless network can be deployed in 3D space. It is not influenced by placement of wormhole. It has smaller communication costs. Multiple wormhole can be well recognized. But there is greater chance of false positives with smaller length of wormhole. It is not suitable for highly dynamic environment. It is difficult to detect when nodes not report malicious behaviour.

It detects suspicious nodes. This strategy can be further improved. Multiple wormhole detection can also be further improved. The number of false positives remains still an open area for closer investigation.

In study of **case study on MANET routing protocols performance over TCP and HTTP**[18] presented by **Yamsani Ravikumar and Sarath Kumar Chittamaru**, the aim is to find out efficient routing protocol for routing among DSR, OLSR and AODV. For this Two scenarios created in NS2 one with 10 nodes and other with 50 nodes. First Impact of scalability on MANET routing protocol performance is taken under consideration. Then Impact of network load on MANET routing protocol performance is measured by creating two scenarios with 50 nodes each with constant speed of 10 m/s but with different profiles one as HTTP heavy load traffic and other as HTTP light load traffic. After that Impact of node mobility on MANET routing protocol performance is measured by creating two scenarios each with 50 nodes with speed of 10 m/s and 28 m/s respectively over 1000mX1000m area. Lastly, Impact of TCP over MANET routing protocol performance have been measured by creating two scenarios each with 50 nodes and HTTP heavy and light load respectively over 1000mX1000m area simulated for each protocol separately for 10sec for two scenarios. The parameters to measure performance is throughput and delay. The author gives very keen knowledge about the current scenarios of considered protocols. It also exploits the research areas where work is needed to be done. But none of the protocol prove efficient. The parameters for comparison is also less. We found that OLSR is scalable and can work in high node mobility also delay is less when load is also less, AODV can handles network load and delay is less even when the load is high. TCP only shows less delay when load is also less.

In literature review, we found that every proposed scheme is lacking in some aspects. A distributed approach is needed to overcome at least some of the current scenario problems.

3. Comparative Analysis

Here is the comparison study on different schemes learnt in this course of study. The techniques which prevent and detect the wormhole attack is AOMDV, AHP, SECUND and LWDP. In TBA and AHP there is high delay whereas in other techniques, the delay is less. The high throughput is given by AOMDV and LWDP, other schemes can perform well but as compared to AOMDV and LWDP other schemes lack throughput.

The AOMDV, AHP and SECUND inculcates high computation overhead whereas other schemes do not need rigorous calculations. Only SECUND and LWDP proves to be supportive in dynamic topology, but AOMDV can also support dynamic topology but to some extent only.

No schemes are suffering from hardware constraints, as no special hardware is required. The SECUND and LWDP are only schemes that are not affected by node mobility, that means it supports dynamic or mobile network.

The SECUND, LWDP and LCT schemes support scalability but other schemes do not. There are only one schemes which is impacted by network load that is AHP. The AOMDV and TBA requires periodic updates for their smooth functionality, which may cause load or overhead on network.

The false positives are high in WRSR and LCT schemes, which may lead to performance degradation of network as well as scheme. The SECUND and LWDP support various network size, but AOMDV support only dense networks and other schemes are suitable for small network. In no schemes, we require cryptography but in SECUND there is need of cryptography.

Table 1. Comparison Table

Parameters	AOMDV	TBA	WRSR	AHP	SECUND	LWDP	LCT
Wormhole detection or prevention	Both	Prevention	Detection	Both	Both	Both	Detection
Delay	Less	High	Less	High	Medium	Less	Less
Throughput	High in dense network	Low	Low	Medium	Medium	High	Medium
Computation Overhead	High	Less	Less	High	High	Less	Less
Support dynamic topology	Minimal	No	No	No	Yes	Yes	No
Hardware constraints	No	No	No	No	No	No	No
Impact of node mobility	Yes	Yes	Yes	Yes	No	No	Yes
Impact of scalability	Yes	Yes	Yes	Yes	No	No	No
Impact of network load	No	Yes	No	Yes	No	No	No
Periodic updates	Yes	Yes	No	No	No	No	No
False positives	Less	Less	High	Less	Less	Less	High
Network size	Dense	Small	Small	Small to Medium	Variable	Variable	Small
Cryptographic mechanism required	No	No	No	No	Yes	No	No

4. Discussions

The comparison table help to summarize the length conclusions. As we can notice that the various schemes are compared on the basis of some parameters. These parameters are basis for a technique or schemes to be effective and useful. The wormhole is focal point of our comparison study and it shows in the table that some techniques prevent or some detect the wormhole attack. Delay is other parameter which tell us the optimality and effectiveness of schemes, lesser the delay more effectiveness. The throughput is the most important of the parameters to check the effectiveness of the scheme. The more the throughput will be, the more effective the scheme will be. The computation overhead arises when schemes involves lots of calculations, if more overhead than more the delay and less effective. As MANET is highly dynamic, we need a scheme which support dynamic nature of network. If network is dynamic that means it will be mobile, so schemes should support the mobility of node as well. The network in MANET created on the fly, so nodes join the network or exit the network, in order to handle this scalability, the schemes should likely to be able to adapt this scalability. The network might be full of load or traffic, the scheme should be capable of handling such loads. Some schemes require periodic updates for their smooth functioning but can degrade performance of network by increasing load on network. the false positive is a factor which might approve the malicious node in the network as a valid node, which is very harmful to network. the number of false positive should be less to prove the effectiveness and optimality of a scheme. Every scheme is suitable for different size of network. The cryptographic mechanism is required for authentication the nodes present in network.

5. Conclusions

In this course of study, we found the comparison of different techniques or schemes based on some parameters. We found that how effective these techniques or schemes can be based on our comparative study. The techniques or schemes taken

under consideration lack in some aspects. They are not fully effective but can be used where in certain circumstances we do not require much of that particular parameters in which it lacks. After this study, we found that no presumed techniques or schemes are optimal. The further research can be done by taking more parameters and by widening or narrowing the research area.

References

[1] A.-S. K. Pathan, H.-W. L. Lee and C. S. Hong, "Security in wireless sensor networks: issues and challenges", 8th International Conference Advanced Communivcation Technology, vol. 2, **(2006)** , pp. 1043-1048.
[2] R. Singh, "Countermeasures against wormhole attack in wireless sensor networks: A Survey", International Journal of Computer Science & Communication Networks, vol. 6, **(2016)** May, pp. 79-84.
[3] M. B. R. Baviskar and M. V. N. Patil, "Black Hole Attacks Mitigation and Prevention in Wireless Sensor Network", International Journal of Innovative Research in Advanced Engineering, vol. 1, no. 4, **(2014)**, pp. 167-169.
[4] D. Mishra, "A Review on Gray Hole Attack in Wireless Sensor Network", International Journal of Computer Applications, vol. 122, no. 2, **(2015)**, pp. 33-36.
[5] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses", IEEE Pervasive Computing, vol. 7, no. 1, **(2008)**, pp. 74-81.
[6] E. V. Ramana, F. Fatima and L Sunitha, "Vampire Attacks in Wireless Sensor Networks : Evaluation and Protection", International Journal of Computer Science and Information Technology Research, vol. 2, no. 4, **(2014)**, pp. 34-38.
[7] N. Mohan and A. Pasha, "Distributed Detection of Byzantine Attacks in WSNs : A Short Critical Survey", International Journal of Computer Science and Information Technology Research, vol. 2, no. 2, **(2014)**, pp. 390-403.
[8] P. Amish and V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", Procedia Computer Science, vol. 79, **(2016)**, pp. 700-707.
[9] N. N. Dangare and R. S. Mangrulkar, "Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network", Procedia Computer Science, vol. 78, **(2016)**, pp. 342-349.
[10] G. Akilarasu and S. M. Shalinie, "Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks", Wireless Networks, DOI:10.1007/s11276-016-1240-0, **(2016)**, pp. 1-10.
[11] R. Matam and S. Tripathy, "WRSR : wormhole-resistant secure routing for wireless mesh networks", EURASIP Journal on Wireless Commununications and Networking, DOI:10.1186/1687-1499-2013-180, no. 180, **(2013)**, pp. 1-12.
[12] S. Banerjee and K. Majumder, "A comparative study on wormhole attack prevention schemes in mobile ad-hoc network", Communications in Computer Information Science, vol. 335 CCIS, **(2012)**, pp. 372-384.
[13] S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks", Ad Hoc Networks, vol. 1, no. 1, **(2003)** , pp. 151-174.
[14] F. Shi, W. Liu, D. Jin and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology", Electronic Commerce Research, vol. 13, no. 3, **(2013)**, pp. 329-345.
[15] T. Hayajneh, P. Krishnamurthy, D. Tipper and A. Le, "Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies", Mobile Networks and Applications, vol. 17, no. 3, **(2012)**, pp. 415-430.
[16] T. Dimitriou and A. Giannetsos, "Wormholes no more? Localized wormhole detection and prevention in wireless networks", Lecture Notes Computer in Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6131 LNCS, **(2010)**, pp. 334-347.
[17] X. Ban, R. Sarkar and J. Gao, "Local connectivity tests to identify wormholes in wireless networks", Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing, **(2011)**, p. 13:1-13:11.
[18] Y. Ravikumar and S. Chittamuru, "A Case Study on MANET Routing Protocols Performance over TCP and HTTP", School of Engineering Blekinge, **(2010)** June.
[19] G. Kumar, M. K. Rai, H. Kim and R. Saha, "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks", Mobile Information Systems, (**2017).**
[20] G. Kumar, M. K. Rai and R. Saha, "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks", Journal of Network and Computer Applications, vol. 99, **(2018)**, pp. 10-16.

