International Journal of Engineering &Technology, *7 (3.12) (2018) 290-295*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

SRDP: Secure Route Diversion Policy for Resisting Illegitimate Request in MANET

H C Ramaprasad[1*], S C Lingareddy[2]

[1]Research Scholar, Visvesvaraya Technological University, Belgaum
[2]Prof, Dept. of CSE, Sri Venkateshwara College of Engineering, Bengaluru, India
**Corresponding Author E-Mail: [1]ramaprasadhc@yahoo.com*

Abstract

Optimized Link Source Routing (OLSR) is currently identified as one of the robust on-demand protocol in Mobile Adhoc Network (MANET) for offering good communication performance. However, there are very less evidence where it is found to support potential security. After reviewing existing security approaches in MANET, it is found that there is a still an open scope of security in MANET where the potential of OLSR can be harnessed. Hence, this manuscript presents SRDP or Secure Route Diversion Policy that is capable of identifying the incoming threat irrespective of any form of attacks. SRDP allows comprehensive identification of threat and it offers safety to the network by further resisting such incoming messages to be propagated within its secured network. The study outcome shows that SRDP offers good communication performance and retain good balance with cost effectiveness in contrast to existing security schemes.

Keywords; *Mobile Adhoc Network, Adversaries, Attacks, Secure Routing, OLSR, Communication*

1. Introduction

In current days, advancement of wireless technology and increasing demand of mobile or smart devices, made wireless networks more popular. MANET (i.e. Mobile Ad-Hoc Network) is an independent wireless network infrastructure which contains self-configurable mobile nodes. MANET is a type of Ad-Hoc network which has significant properties such as 1) Distributed network, 2) Dynamic topology, 3) wide network boundary, 4) fast implementation and 5) node by node communications [1]. Due to these features and increasing demand of MANET facing several challenges e.g. integration with internet, managing network topology and security. As per the research study, MANETs has several security problems, because these are more vulnerable to security hazards than wired networks [2]. In MANETs, all the nodes are totally depending upon battery-power for their operation. The alternative energy resources are may be unavailable. The adversary node can forward a more traffic to the destination node. The destination node might be busy in managing these data packets; this leads to battery life time to be exhausted. However, the scalability of MANETs always keeps on changing. It is more challenging task to predict number of available nodes in the mobile networks for future time. The protocols designed for mobile ad-hoc networks must be developed compatible for this changing scalability. In small infrastructure networks it is hard task to handle security problems as every node is able to move in any direction and there is non-centralized security provisioning in such kind of networks. In MANET's attacks are majorly classified into 2 categories i.e. 1) Active attacks (e.g. Denial of Service attacks) which try to disrupt the network functionality by reading or changing the information of packets, and 2) Passive attacks (i.e. Route tracing attack) which do not interrupt the network functionality.

The finding of passive attack is more complicated compared to active attacks. These attacks are furthermore divided into 4 different categories like i) Attacks occurring via modifications (e.g. Re-directions by updating rout sequence number, hop count, DoS by changing source routing and Tunneling), ii) Spoofing (i.e. impersonation attacks) where malicious node alters its IP/MAC address for outgoing packets and exploits another node address. iii) Attacks utilizing Fabrication (e.g. overflow of routing table attacks, falsifying routing error message), iv) Rushing attacks which are applicable only upon on demand routing protocol where only single request packet is send to discover the route to target node. Based on research study [3], MANET's security routing protocols can be categorized as 1) Prevention and 2) Detection and Reaction. Further, these routing protocols are divided into several categories. The prevention routing protocol mainly contains symmetric and asymmetric cryptography scheme which is based on route querying method and cryptographic certification method respectively. Additionally, this category also include one directional hash cyclic approach which is responsible to manage efficient and secure Ad-Hoc distance-vector routing system where it checks the authenticity of the data-packet and forwards the routing updates. Whereas Detection and Reaction routing scheme include "Byzantine", "Watchdog and Pathrater" protocol. The Byzantine algorithm primarily utilized to prevent the network topology from byzantine failures (i.e. dropping packets, attacks occurred from malicious nodes etc.). Therefore, this research work introduces an approach that is capable of addressing the security problems in MANET in more efficient and novel manner. The emphasis of the paper is towards cost effectiveness and non-incorporation of conventional cryptographic measures. The rest of the research study is organized as; section-II reviews about existing work carried out in MANET security system. Section-III illustrated about problem identification.

While, section-IV and V discusses the research methodology and algorithm description followed by result analysis in section-VI. Finally, the study ends with conclusion and future scope.

2. Related Work

This section briefs of the existing security approaches in MANET. The Work of Alocious et al. [4] have conducted an analytical study of Misbehaviors of Mac layer under DoS attack with IEEE 802.11 protocol in the MANETs Surroundings. The outcome of the study display that the DoS attack on MAC layer degrades the performance of network in terms of throughput and higher data packet loss rate. A game theory based concept is used in the work of Amraoui et al. [5] and designed an innovative model that provides interaction between behaviors of nodes and a cooperative track-record table is used by the every node to deal with selfish behavior of destructive nodes. Kandah et al. [6] have tried to introduce the behavior of adversary that initiate a Colluding attacks on nodes which aims to disturb the packet transmission process with hiding their identity and existence and in the same way Moudni et al. [7] have studied and investigated the performance of AODV routing protocol under various attacks and it is found that of impact of attacks decreases the performance of MANET. Pravin et al. [8] have examined the impact of DoS attacks and gave a novel method of packet filtering that works to detect compromised nodes and to enhance the performance of operational functionalities of networks. Qin and Huang [9] have designed a new strategy based on position based routing approach that compromise the transmission anonymity of MANET and identifies end-to-end flow between source and destination with maximum accuracy. The work carried out by Sharma and Jain [10] have concentrated the impact of wormhole Attack in MANET with aim to derive various strategic steps to identify and prevent the mobile nodes from such types of attacks. The work of Shrestha and Nam [11] have, used vector quantization approach in VANET to reduce the effect malevolent vehicles in respect to trust level to other vehicles. The Silva and Albini [12] have presented a middleware concept that performs processing, security and services, task that helps to build security decision making strategy. In the study of Singha and Das [13] have, conducted an elimination and detection methods by using Cryptographic concept to enhance the energy utilization in nodes and to prevent the network topology form various security threats.

The work carried out by the Arya and Rajput [14] have presented a secure and robust model of AODV routing protocol by using secret-key authentication and key distribution method. The outcomes of study delivers that present approach achieves effective performance over existing approaches. The work of Douss et al. [15] have presented an improved trust based clustering algorithm which supports to build the trust among different networks in order to boost the overall performance of network components and to reduce the other nodes getting destructive. Gawande and Suryavanshi [16] have presented a new on demand routing based on the cryptographic technique to secure and enhance the functional property of MANETs. A new trust based routing protocol is proposed by Jawhar et al. [17] for the MANETs and other sensor networks which discover secure multi-hop path between the source node and the destination node at the time of data transmission process by which security is increased in communication layer of networks. Narayanan and Radhakrishnan [18] have targeted the black hole attack that launched on the direct root of packet transmission which causes packet dropping factor and data traffic collision. The author [19] has presented an improved AODV protocol routing method with using MAC layer by which nodes have to prove their reliability. The outcomes of this study display the presented approach is able to defend the network from the Black-hole attacks and achieves good throughput and packet delivery rate. Another work of Work of Wu et al. [20] have provided a model that use to perform measurement task for the MANET resilience factor with fault tolerance strategies and also conducted a study to analyze the factor that influences the resilience property. In the study of Xia and Pan [21] have focused on various security issues in MANETs and presented a decentralized trust model depends on the node's behavior judgment. The result of this study shows the presented model provides good security features with low computational overhead and also the model obtains flexible property that it can be integrate with some traditional security approaches.

There are also reported study where Optimized Link Source Routing (OLSR) is adopted to offer security in MANET. The work carried out by Amraoui et al.[22] have emphasized on addressing the security problems associated with selfish behaviour of a node. The study outcomes are validated using data rate, delay, and routing protocols; however, there was no benchmarking the outcomes. Ben-othman and Benitez [23] have added signature-based scheme using encryption mechanism to offer security in HELLO and TC (topology) control messages in OLSR. Bowitz et al. [24] have developed BATMAN protocol that is claimed to offer better security than OLSR; however, there is no empirical evidence to prove this claim in its analysis. Jeon et al. [25] have modified conventional OLSR to make it resistive against link replication attacks. The work carried out by Schweitzer et al. [26] have used OLSR to address the problems associated with gray hole attack in MANET using simulation-based approach. Joint approach of asymmetric cryptography and OLSR protocol was adopted in the work of Semchedine et al. [27]. Snoussi et al. [28] have implemented an approach where clustering concept is utilized for identifying threats in MANET when it uses OLSR protocol. The study carried out by Villalba et al. [29] have also modified the OLSR protocol in order to incorporate security feature in it. The technique is meant for identifying the malicious behaviour of attacker in MANET.

Hence, it can be seen that there are various existing approaches towards security MANET with associated advantages as well as issues too. The next section outlines the research problems.

3. Problem Identification

After reviewing the existing system, it has been seen that there are various approaches towards securing MANET communication system. However, following are the problems that has been identified in the existing system:

- Narrowed Performance Score: A closer look into the existing outcomes will shows that majority of the approaches are designed on the basis of sniffing-based, encryption-based, authentication-based, routing-based, etc. All these techniques are associated with higher processing time, delay, no centralized governance, increased overhead, etc. Lack of benchmarking is another significant problems associated with existing system.
- Attack-Specific Solution: Almost all the approaches introduced till date on MANET security is constructed on the basis of specific forms of attack. Some of the attacks that has received more attention are denial-of-service attack, rushing attack, routing table tampering attack, etc. However, other forms of attacks have received very less attention. Each attacks has their own strategy to launch adversary, which has not been found to be realized in MANET secure routing protocols.
- Lack of Compliance of security standards: It is essential that existing secure routing protocol in MANET offers theoretical claim of various security standards e.g. authentication, integrity, central trust authority, non-repudiation, confidentiality, availability, etc. However, a closer look into any research towards security solution in MANET is found not to prove this fact apart from authentication and privacy issues. A closer analysis of security performance of many security protocols will show that they do not have much supportability against availability and integrity. Hence, it will conclude the fact that none of the existing security solution in MANET are completely resilient against all threats.

- Less work on OLSR: Irrespective of lots of advantages features of OLSR, it is still shrouded by issues that calls for security problems in it. Some of the charecteristics e.g. i) maintenance of routing information increases security threats that calls for single hop-based security and not multi-hop based security, ii) increase of overhead with maximization of the mobile nodes leads to scenario of man in middle attack, and iii) involvement of more processing time that results in delay and possible invitation to some lethal threats.
- Uncertainty of identifying the incoming request: At present, there are few solution that is capable of identifying the degree of threats from the incoming request from neighboring nodes. Lack of identification as well as lack of uniform update policy of secure routing also causes inability to identify the nature of threat in MANET.

Therefore, all the above mentioned problems are considered as significant problems in MANET. Therefore, the proposed system intends to solve the above mentioned unsolved security problems in MANET in order to bridge the research gap as well as trade-offs in existing security approaches.

4. Research Methodology

The proposed system develops a novel analytical model SRDP that is meant for identifying any form of illegitimate request in MANET environment. With reference to Fig.1, the proposed scheme construct a master hop records for each communication that are successfully completed by regular node. This also acts as trust-based information for regular nodes where the trust factor is maintained with respect to single and multiple hops. Inspite of directly applying conventional OLSR, the proposed system offers slight change in its mechanism of forwarding HELLO and TC (Topology Control) information. According to the new scheme, this information will be forwarded to regular node, but decision that the incoming request is originating from regular or unknown node will be decided by a new node called as route diversifier node. It runs a special form of algorithm where it always rejects TC message from any node that are not listed in its hop record. At the same time, the route diversifier node checks if the destination node falls under multiple hop. The logic is to ensure that many numbers of nodes should be compromised and for this purpose the route diversifier node forwards a unique message against which only regular node could perform validation. It is obvious that malicious node will assume route diversifier node a normal mobile node and forward its forged information which will violate the information retained within hop record. This mechanism is simpler and faster way to identify malicious node and their illegitimate request., which upon receiving, route diversifier forward forged information so that malicious node spend its resources unnecessarily to search for this forged routes.

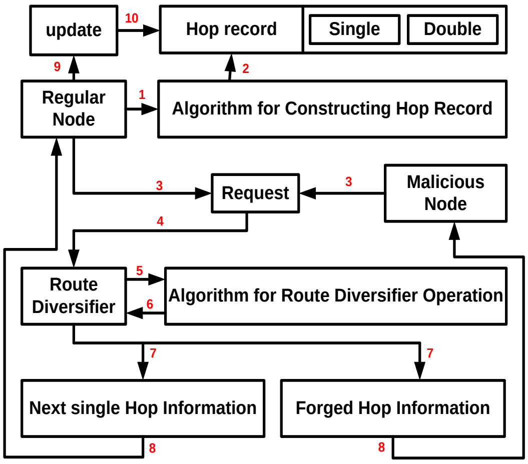

Fig. 1: Proposed Research Methodology

Therefore, the contribution of the proposed system is a follows viz. i) The primary contribution of the proposed system is to formulate a route diversion attack in MANET using analytical research methodology, ii) The secondary contribution is also to revise the mechanism of conventional OLSR routing mechanism in order to incorporate more level of security, and iii) The tertiary contribution of proposed system is to develop a cost effective secure routing using non-cryptographic approach. The next section discusses about the algorithm implementation of proposed system.

5. Algorithm Description

The prime purpose of this algorithm is to offer resistivity to the diversion-based attacks in MANET. The design of the algorithm is also created in such a way that it will invoke equivalent resistivity to any other forms of threats to mobile nodes in MANET. In order to implicate security, the proposed system implements two core algorithms i.e. algorithm for constructing hop records and algorithm for route diversifier operation. The discussion of the algorithm is as follows:

A. Algorithm for Constructing Hop Records

This algorithm is responsible for constructing hop records that is maintained for all the mobile nodes. The information containing within this is highly essential to carry out authentication of mobile nodes. This algorithm takes the input of s (simulation area), n_c (node concentration), s_r (sensing range), and n (number of nodes) that after processing leads to an outcome of h_r (hop record). The steps of the algorithm are as follows:

Algorithm for Constructing Hop Record

```
Input: $s, n_c, s_r, n$
Output: $h_r$
Start
1. init s, $n_{c,}$ $s_r$
2. For i=1: n
3.   $h_r$→$f_1$(pos, n, s, $s_r$)
4.   For j=1:n-1
5.     [$x_1$ $y_1$]→[$x_j$ $y_j$]
6.     For k=j+1:n
7.       [$x_2$ $y_2$]→[$x_k$ $y_k$]
8.       $d=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$
9.       If d>0
10.        If d≤$s_r$
11.          $h_r$(j,k)=1
12.        End
13.      End
14.    End
15.  End
16. For $l$=1:$n$-1
17.   unit link→explore($h_r$($l$)==1)
18. End
19. End
End
```

The algorithm after initialization (Line-1) considers all the deployed mobile nodes for constructing hop record (Line-2). For this purpose, a special function f_1(x) is constructed that takes in the input of position of nodes, number of nodes, simulation area, and sensing area (Line-3) in order to create a matrix h_r for hop record. The algorithm also emphasis on considering all the links existing between source to destination node (Line-4) which offers frequent update of new position of mobile nodes (x_1, y_1) from its old position (x, y) corresponding to the source mobile node (Line-5). With every change in hops, it also record the node position with respect to the change of hops (Line-6) in the form of (x_2, y_2). Hence, (x_2 y_2) represents new hop position while (x_1 y_1) represents old hop position while (x y) represents original (static) position of mobile node (prior to deployment). The hop distance is computed using Euclidean distance (Line-8). In case of positive hop distance (Line-9), the algorithm checks if the newly obtained hop distance is less than sensing range (Line-10). If the newly obtained hop distance is less than the sensing range than it is indexed as unit value or else it may take any other value starting from 0 to less than 1. The prime logic behind this is to differentiate malicious node to regular node in MANE. Usually, malicious node will not like to be within the sensing range for a long period of time in case if it has any prior attack history whereas it is certain that regular node will always try to reside within the sensing range. A closer look into this algorithm also shows that a matrix for hop record is constructed by only for single hops for all communicating links and not for multi-hops. It will mean that the algorithm restores all the hop information between two communicating nodes (Line-17) and only unique hop list is used. This hop table is used by all the mobile nodes in order to confirm the legitimate routing history before establishing the communication with requestor node.

B. Algorithm for Route Diversifier Operation

The prime task of this algorithm is to offer resistance against illegitimate request. The algorithm is responsible to create diversion of route for any form of illegitimate request it extracts. The algorithm takes the input of *req* (number of request) that after processing yields *msg* (acceptance/diversion message).

```
Algorithm for Route Diversifier Operation
Input: req
Output: msg
Start
1. For i=1: req
2.   If req= = TC($h^{+2}$)
3.     $n_{rd}$→msg($x_3$ $y_3$)|( $x_3$ $y_3$) doesn't exists in $h_r$
4.   Else
5.     $n_{rd}$ checks $n_{nodes}$(requestor)
6.     If ($n_{nodes} \subseteq h_r$)
7.       $n_{rd}$→msg($x_3$ $y_3$)|( $x_3$ $y_3$) doesn't exists in $h_r$
8.     Elseif $n_{rd}$→msg($x_1$ $y_1$)
9.     End
10. End
End
```

The algorithm initially allows route diversifier node n_{rd} to assess all the incoming request *req* (Line-1). It typically looks for any request with topology control message TC that relates to more than two hops (Line-2). Such forms of message are considered as malicious program and n_{rd} forwards a forged message with forged route information with next node (x_3, y_3) that never existed in h_r (Line-3). However, if the incoming request not a TC message (Line-5) than n_{rd} checks for the neighbor node n_{node} information of the requestor node (Line-6). A positive match (Line-6) will allow nrd to repeat its process of forwarding similar forged information to illegitimate node (Line-7). If none of these conditions are satisfied, it will represent that the requestor node is regular node and they are forwarded only next node information by n_{rd} (Line-8).

6. Result Analysis

This section discusses about the outcomes obtained from the proposed implementation of SRDP. Being scripted in MATLAB, the proposed system uses 500-1000 mobile nodes spread randomly over 1100 x 1300 m^2 simulation area. As the proposed solution is claimed to be an enhanced version of conventional OLSR routing protocol for offering better security features, the initial assessment is carried out using delay minimization and throughput. Fig.2 highlights that SRDP offers approximately 20% of improvement in delay minimization as compared to existing OLSR protocol. The prime reason behind this is SRDP offers initial checks on various conditions of legitimacy of incoming request before even processing that request unlike conventional OLSR. At the same time, the algorithm supports good non-repudiation that can be observed through the performance of throughput (Fig.3).

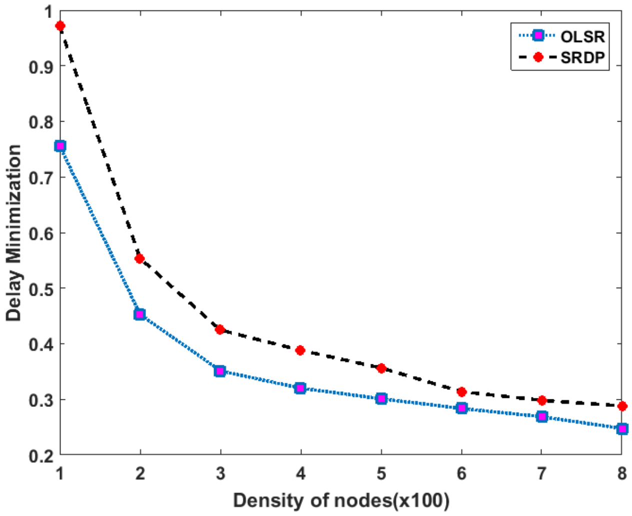

Fig. 2: Analysis of Delay Minimization

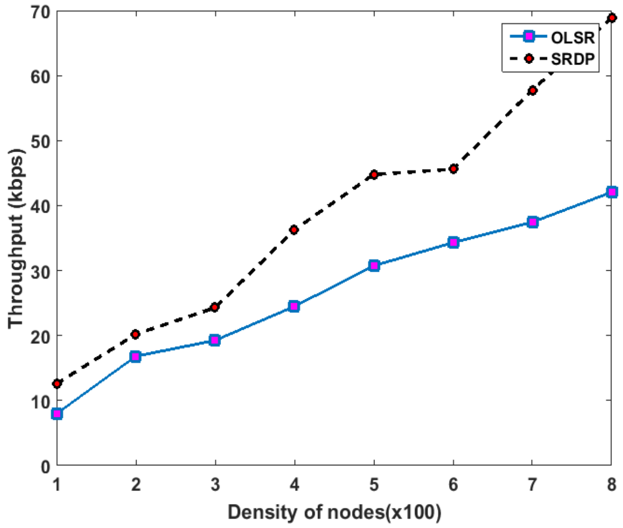

Fig. 3: Analysis of Throughput

Further, for an effective benchmarking, SRDP is compared with existing routing mechanism e.g. .SAR [30], ARAN [31], SRP [32], SEAD [33], SLSP [34], SAODV [35], SA-OLSR [36] In order to perform this analysis, the study considers packet size of 2000 bytes to be forwarded in presence of unknown number of attackers. Similar test bed has been used for assessing the performance. Table 1 highlights the comparative analysis to prove that proposed SRDP offers faster response time, with good delivery of data packets, and doesn't offer any form of computational / network overhead.

Table 1: Comparative Analysis

Approaches	Processing time (sec)	Throughput (kbps)	Overhead (bytes)
SAR [30]	3.2114	1127.38	1127.51
ARAN [31]	3.9882	1522.56	1272.09
SRP [32]	4.1671	7789.21	1782.08
SEAD [33]	1.5391	8098.13	9029.65
SLSP [34]	5.9799	5287.1	1672.11
SAODV [35]	4.2851	1254.09	1178.87
SA-OLSR [36]	0.9227	1772.43	789.09
SRDP	0.3766	1901.23	305.54

The prime reason behind the performance of the proposed system is that it doesn't have any form of recursive principle involved while offering security features unlikely any cryptographic algorithms of existing system. Another reason for the better performance is that SRDP allows formation of secure hop records which makes the task easier to cross-validate the form of incoming request from unknown node. Further layer of security is maintained by offering only node information present in one hop and not more than that. Once this new hop is used for communicating with the new requestor node, their neighborhood information along with trust factor is recomputed to confirm if it is really a regular node or latent attacker node. Hence, without usage of any complex cryptographic method, the proposed system offers cost effective security options for MANET irrespective of any forms of attacks.

7. Conclusion

Security in MANET is still an ongoing problem while there is less number of significant research using OLSR protocol for incorporating security. This gap is bridged by introducing SRDP that is capable of identifying the malicious threat and can govern their behaviour. Different from existing approaches of intrusion detection/prevention system, SRDP offers forged information to the attacker node once positively identifying them as adversary. This phenomenon directly affects the resources of attacker by initiating / formulating attacking strategy to the recently obtained forged information from route diversifier node. The study outcome shows that proposed system offers a good communication cycle as well as it is also found to be computationally cost efficient. Our future work direction will be to further optimize its features.

References

[1] Jonathan Loo, Jaime Lloret Mauri, Jesús Hamilton Ortiz, “Mobile Ad Hoc Networks: Current Status and Future Trends”, CRC Press, 2016.

[2] A. L. Sandoval Orozco, J. García Matesanz, L. J. García Villalba, “Security Issues in Mobile Ad Hoc Networks”, SAGE-JOurnals, International Journal of Distributed Sensor Networks, 2012

[3] A. Vij and V. Sharma, “Security issues in mobile adhoc network: A survey paper”, IEEE International Conference on Computing, Communication and Automation (ICCCA), Noida, pp. 561-566, 2016.

[4] C. Alocious, H. Xiao and B. Christianson, “Analysis of DoS attacks at MAC Layer in mobile adhoc networks”, 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015, pp. 811-816.

[5] H. Amraoui, A. Habbani, A. Hajami, and E. Bilal, “Research Article Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model”, Hindawi Publishing Corporation, pp. 17, 2016

[6] F. Kandah, Y. Singh and Chonggang Wang, “Colluding injected attack in mobile ad-hoc networks”, 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, pp. 235-240, 2011.

[7] H. Moudni, M. Er-Rouidi, H. Mouncif and B. El Hadadi, “Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks”, 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, pp. 385-389, 2016.

[8] S.Parvin, F. K. Hussainb and S. Ali, “A methodology to counter DoS attacks in mobile IP communication”, Mobile Information Systems, pp. 127-152, 2012.

[9] Y. Qin and D. Huang, “Least Squares Disclosure Attack in Mobile Ad Hoc Networks”, 2011 IEEE International Conference on Communications (ICC), Kyoto, pp. 1-5, 2011.

[10] M. Sharma, A. Jain and S. Shah, “Wormhole attack in mobile ad-hoc networks”, 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, pp. 1-4.2016.

[11] R. Shrestha and S. Y. Nam, “Research Article Trustworthy Event-Information Dissemination in Vehicular Ad Hoc Networks”, Hindawi Mobile Information Systems, pp. 16, 2017

[12] E. d. Silva and L.C.P. Albini, “Research Article SEMAN: A Novel Secure Middleware for Mobile Ad Hoc Networks”, Hindawi Publishing Corporation, pp. 18, 2016.

[13] S. Singha and A. Das, “Detection and elimination of the topological threats in mobile ad hoc network: A new approach”, 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, pp. 907-911, 2015.

[14] K. V. Arya and S. S. Rajput, “Securing AODV routing protocol in MANET using NMAC with HBKS technique”, 2014 International Conference on Signal Processing and Integrated Networks (SPIN), Noida, pp. 281-285, 2014.

[15] A. B. C. Douss, S. Ayed, R. Abassi, N. Cuppens and S. G. E. Fatmi, “Trust Negotiation Based Approach to Enforce MANET Routing Security”, 2015 10th International Conference on Availability, Reliability and Security, Toulouse, pp. 360-366, 2015.

[16] P. D. Gawande and Y. Suryavanshi, “Cryptography based secured advanced on demand routing protocol in MANET's”, 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, pp. 1478-1481, 2015.

[17] I. Jawhar, F. Mohammed, J. A. Jaroodi and N. Mohamed, “TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks”, 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, pp. 382-387, 2016.

[18] S. S. Narayanan and S. Radhakrishnan, “Secure AODV to combat black hole attack in MANET”, 2013 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, pp. 447-452, 2013.

[19] U. Singh, M. Samvatsar, A. Sharma and A. K. Jain, “Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol”, 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, pp. 1-6, 2016.

[20] W. Wu, N. Huang, L. Sun, and X. Zheng, “Research Article Measurement and Analysis of MANET Resilience with Fault Tolerance Strategies”, Hindawi Mathematical Problems in Engineering, pp. 10, 2017

[21] H. Xia, J. Yu, Z. Y. Zhang, X. G. Cheng and Z. K. Pan, “Trust-Enhanced Multicast Routing Protocol Based on Node's Behavior Assessment for MANETs”, 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, pp. 473-480, 2014.

[22] H. Amraoui, A. Habbani and A. Hajami, “Effect of selfish behaviour on OLSR and AODV routing protocols in MANETs”, 2014 Global Summit on Computer & Information Technology (GSCIT), Sousse, pp. 1-6, 2014.

[23] J. Ben-othman and Y. I. S. Benitez, “A new method to secure RA-OLSR using IBE”, 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, pp. 354-358, 2012.

[24] A. G. Bowitz, E. G. Graarud, L. Brown and M. G. Jaatun, “BatCave: Adding security to the BATMAN protocol”, 2011 Sixth International Conference on Digital Information Management, Melbourn, QLD, pp. 199-204, 2011.

[25] Y. Jeon, T. H. Kim, Y. Kim and J. Kim, “LT-OLSR: Attack-tolerant OLSR against link spoofing”, 37th Annual IEEE Conference on Local Computer Networks, Clearwater, FL, pp. 216-219, 2012.

[26] N. Schweitzer, A. Stulman, R. D. Margalit and A. Shabtai, “Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks”, in IEEE Transactions on Mobile Computing, vol. 16, no. 8, p. 2174-2183, Aug. 1 2017.

[27] F. Semchedine, A. Moussaoui, K. Zouaoui and S. Mehamel, “CRY OLSR: Crypto Optimized Link State Routing for MANET”, 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, pp. 290-293, 2016.

[28] Y. Snoussi, J. M. Robert and H. Otrok, “Novel detection mechanisms for malicious attacks targeting the cluster-based OLSR protocol”, 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Wuhan, pp. 135-140, 2011.

[29] L. J. G. Villalba, J. G. Matesanz, D. R. Canas and A. L. S. Orozco, “Secure extension to the optimised link state routing protocol”, in IET Information Security, vol. 5, no. 3, pp. 163-169, September 2011.

[30] Seung Yi, Prasad Naldurg, Robin Kravets, “Security-Aware Ad hoc Routing for Wireless Networks”, In Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001.

[31] Kimaya Sanzgiri , Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields, “A Secure Routing Protocol for Ad Hoc Networks”, In 10 Conference on Network Protocols (ICNP), November 2002.

[32] P. Papadimitratos, Z.J. Haas, P. Samar, “The Secure Routing Protocol (SRP) for Ad Hoc Networks”, draft-papadimitratossecure-routing-protocol-00.txt 2002-12-11

[33] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, “SEAD:Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, In 4th IEEE Workshop on Mobile Computing Systems & Applications, 2002.

[34] P. Papadimitratos and Z. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks”, In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[35] Manel Guerrero Zapata , and N. Asokan, “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing”, ACM Mobile Computing and Communications Review, vol. 3, no. 6, 106-107, July 2002, pp.

[36] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, “SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks”, 2008 IEEE International Conference on Communications, Beijing, pp. 1464-1468, 2008.