SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Mobile Ad Hoc Networking Issues and Challenges: A Review of Related Literature

Ferdinand V. Dalisay
Pangasinan State University
fvdalisay@psu.edu.ph

Abstract - *MANET has the following characteristics: "open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications". These features made MANET vulnerable to different issues and challenges. This paper outlines the different issues and challenges in MANET and are categorized as follows: (1) security, (2) routing, (3) topology control and (4) energy efficiency. A comprehensive analysis of several research papers discussing the issues and challenges, categorized per area, is presented.*

Keywords: MANET, mobile ad hoc networks, MANET security issues and challenges

1. INTRODUCTION

In 1970, the first wireless network was developed in University of Hawaii and was used to wirelessly communicate data across the Hawaiian Islands. But only in 1991 that the Institute of Electrical and Electronics Engineers (IEEE) has formally started standardizing the wireless technologies. in 1997, the first wireless technology standard was ratified by IEEE – the 802.11 [1].

Since then, there was a significant increase in the availability of off-the-shelf wireless technologies that are able to provide wireless and direct connection among user devices. Examples of these wireless technologies are (1) Bluetooth (IEEE 802.15.1) intended for personal area networks and the several 802.11 standards (802.11a/b/g/n/ac) used for high-speed wireless local area networks (WLAN).

WLAN and WPAN can both operate in an infrastructure- less networks where connected devices communicate without the need for any network infrastructure [2]. The network standards indicated above allow devices in the network to directly communicate to other network devices, thus making a single-hop ad-hoc network as shown in Figure 1.

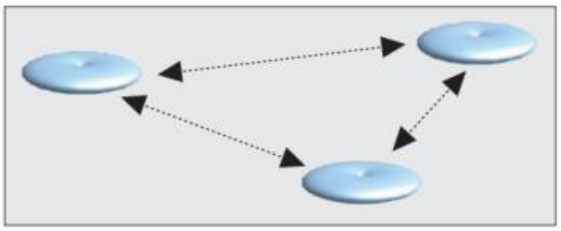

Figure 1: Single-hop Ad hoc Network

An ad-hoc network [3] is a type of network that does not rely on a pre-existing infrastructure such as routers or access points as shown in Figure 2. While in an Infrastructure-based network, devices need to use an access point to control the wireless communication as shown in Figure 3.

Figure 2: Ad hoc Mode

SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Figure 3: Infrastructure-based Network

To extend the capability of an Ad hoc network to communicate with any couple of network nodes, but still without the need of any network infrastructure, the mobile (multi-hop) ad hoc network (MANET) paradigm was conceived by the Institute of Electrical and Electronics Engineers (IEEE) [4]. Mobile Ad Hoc Network (MANET) is a type of an Ad hoc network.

Mobile Ad Hoc Network (MANET) is an "infrastructure- independent network with wireless mobile nodes" [5]. It is composed of wireless nodes that communicate not only to exchange data but also to relay the traffic to other network nodes that cannot directly communicate to each other. To achieve this, any device (or mobile node) in the MANET can act or work as a router to forward packets to the other nodes [6]. MANET is a highly-adaptive network and is rapidly-deployable. Mobile nodes in MANET use a radio broadcast medium for communication.

MANET has the following characteristics [5]: "open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications". These characteristics has made MANET a popular network used in crisis/disaster management [7] [8], disaster recovery [9] [10] [11] [12] [13] [14] [15], medical applications [16] [17], crowdsourcing [7] and for military operations [18] [19] [20] [21]. The special characteristics and features of MANET made it face several issues and challenges.

The study conducted by A. Dorri, S.R. Kamel and E. Kheyrkhah [5] listed the areas of which MANET has the most challenges: (1) security, (2) routing, (3) topology control, and (4) energy. The paper analyzed and discussed the 4th area, the security issues. The different security challenges were discussed and categorized according to 2 different aspects namely: security services and security attacks. However, the paper was not able to cover the other three equally important areas in which MANETs are challenged.

This paper aims to analyze and discuss the existing issues and challenges of the Mobile Ad hoc Network (MANET). The issues and challenges will be categorized in 4 areas, specified by the paper of A. Dorri, et. al. To differentiate this paper from the security challenges discussed by A. Dorri, et. al., the security issues that will be discussed in this paper will only cover the challenges which are documented from 2015. The next section will discuss how this literature review is done. The third section will discuss the results and findings. Finally, the last section concludes the paper.

2 METHODOLOGY

This paper uses a review of related literature to explore published journals and literatures regarding issues and challenges in Mobile Ad hoc Networks (MANETs). The following are the steps undertaken in doing the literature review:

2.1 General database search

Related keywords were used for a general database search. The keywords are: "mobile ad hoc network issues", "mobile ad hoc network challenges", and "MANET issues". The keywords listed above were used in the following academic databases and search engines: Google Scholar, and ACM Digital Library. The search result from the general database search will be initially filtered by the publishing year. All journal articles and papers published from 2012 up to present will be

SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

included in the initial list of literatures to be reviewed.

2.2 Filtering and Analysis of the Results

The initial list of literatures will be reviewed according to its relevance to the research topic. Reading all of the papers and research articles from the results of a general database search can be a very tedious task and may not be feasible because of time constraints. Thus, it was determined that reading the abstract and conclusion is a more realistic approach in filtering the results. A lot of considerations were taken into consideration since the search results also included FANETs, VANETs, WSNs and WMNs which are not synonymous with the term MANETs.

After reading the abstract and conclusion of the researches and literatures from the filtered list, it must also be evaluated according to its relevance to the main research question of this paper: what are the issues and challenges in MANETs?

3 RESULTS AND DISCUSSION

3.1 Results of general database search

Table 1 shows the initial search results for each of the three search queries formulated. The search query "mobile ad hoc network issues" returned the most search results from the three keywords, both in Google Scholar and ACM Digital Library.

Table 1: Number of search results per query

Search Query	**No. of Search Results (Google Scholar)**	**No. of Search Results (ACM Digital Library)**
mobile ad hoc network issues	**1,400,000**	**256,819**
mobile ad hoc network challenges	**684,000**	**157,327**
MANET issues	**67,200**	**166,167**

To further narrow down the number of search results, it has been filtered by publication year. Table 2 shows the number of search results after filtering by publication date.

Table 2 : Number of search results per query

Search Query	**No. of Search Results (Google Scholar)**	**No. of Search Results (ACM Digital Library)**
mobile ad hoc network issues	**39,200**	**88,149**
mobile ad hoc network challenges	**25,900**	**71,029**
MANET issues	**18,500**	**45,772**

3.2 Results of Filtering and Analysis of the Results

The number of filtered results in Table 2 has been further refined by excluding the search results with the terms FANETs, VANETs, WSNs and WMNs. The first page of each search result per keywords has been analyzed. After careful analysis, the search results from the first keyword set returned the most relevant studies. Therefore, the first set of keywords will be used in the next stage of filtering. Next, the search setting is set to only search for papers with the exact keywords in their titles. The query returned

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

48 search results. To get the new security issues of MANET from the filtered list, the keywords "mobile ad hoc network security issues" has been used. The query returned 12 results for the security issues. Out of 12 papers, only 5 provided a full-text for their paper.

There are several issues and challenges found in ths implementation of Mobile Ad Hoc Networks (MANETs). These issues and challenges were summarized in Table 3 and are arranged according to the areas specified by Dorri, namely: (1) security, (2) routing, (3) topology control, and (4) energy.

Table 3: Category of each research paper

No.	Type of Issue	Research
1	security	[51] [52] [53] [54] [55]
2	routing	[3] [15] [16] [17] [27] [29] [30] [31] [36] [37]
3	topology control	[38] 39] [40] [39]
4	energy	[15] [16] [17] [20] [21] [41] [42] 43]

From the list of relevant studies and literatures, the most common type of issue discussed is the security. Security is always the priority when network connections are involved. Just like any other type of network infrastructure, Mobile Ad Hoc Networks (MANETs) face several security issues that arise from MANETs self-configuration and self- maintenance capabilities. Also, all nodes in MANET are free to join and leave the network (also called open network), this characteristic made MANET vulnerable to security-related attacks.

Furthermore, all intermediate nodes between a source node
and the destination node take in part routing, and have the role of forwarding packets to the destination node. This characteristic of MANET will make any node receive a packet which is either destined to it or not. Therefore, malicious behavior can happen if an infected node gained access to a packet then it might inject fault packets to the network. Security has become the most important challenge in MANETs.

Aside from security, there were 8 literatures that discuss routing issues, 6 papers discuss energy issues and 3 papers discuss topology controls. The next section discusses the results of each are in detail.

3.1 Security

Kumar and Babu [51] include several new security attacks that were not included in the paper of A. Dorri, et. al. One attack is called New Comer attack. In this type of attack a malicious node may remove their bad reputation by registering to the network as a new user. The node simple eaves the network and joins again for trust revocation, this way the old bad records for the node will be discarded. This issue was not yet present at the time of Dorri's paper writing since there were no trust management schemes yet at that time. Some other new attacks that were recorded include the following: Sybil attack, replay attacks, on-off attacks, on-off attacks and conflicting behavior attack.

The new attacks that were discussed by Kumar and Babu [51] were also specified as security threats in the paper of Nithya, et. al. [52] Additionally, the issues were presented in the way they affect the OSI Layer. The said issues in the first paper [51] were categorized in the second paper [52] as Application Layer attacks.

SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Compared to other papers reviewed, Gharehkoolchian's paper [53] provided trade-off between routing protocols and security. He pointed out that the routing protocols are the most vulnerable area in which MANET is challenged in terms of security. MANET does not have typical routers for routing in the network. Instead, each node in the network acts or functions as a router. He explained that since every node acts as a router, any node can compromise the routing protocol which can cause security vulnerability. In the same paper, Gharehkoolchian also introduced a modified version of AODV routing protocol to mitigate security holes.

Kulkarni [54], however, said that the clustering can mitigate more of the security issues. Clustering is the process of dividing the network into different virtual groups based in rules. Clustering can restrict the spreading of incorrect information injected in the network by a malicious node.

Surprisingly, Singh and Kumar [55] still documented the same attacks that were discussed in Dorri's paper. Malicious node attack proves to be a very common issue in MANETs [24-26]. Also, black hole attacks were also included in the list [51]. Lo and Li's paper [27] discussed a new type of black hole attack, he called it a cooperative black hole attack. In this attack, at least two malicious nodes are serious security threats. Singh and Kumar [55] classified those attacks as attacks in the Network Layer of the OSI. Black hole attack is an attack where the malicious node injects fault routing information to the network, it also discards all packets sent to it [27]. In addition, Byzantine attack was still a prevalent issue until now. Several papers [28] [29] [30] have already discussed the Byzantine attack. In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop.

However, Singh and Kumar [55] did not already include the Denial of Service and Gray hole attacks in their list of security issues and challenges.

From the literatures reviewed so far, we can conclude that in the area of security, the most attacked layer of the OSI is the Network and Application layers. And compared to the previous years, the abundant researches in mitigating DoS and gray hole attacks were proven effective. However, new problems are continually being discovered such as New comer attack, Sybil attack, replay attacks, on-off attacks, on-off attacks and conflicting behavior attack. It is also worth noting that the attacks that were previously documented were still a problem until today, these include the black hole and malicious node attacks. This indicate that the proposed solutions to mitigate those problems were not very effective.

3.2 Routing

The paper of Dhenakaran [3] correlates the complexity of MANETs topology to the routing protocols. The mobility nature of the nodes in MANET increases the complexity of the routing protocols and the degree of connection's flexibility. He also stated that this flexibility also imposes security risks.

The paper [15], however, linked the routing protocols to some energy usage issues. Macone, et. al. [15] introduced an energy-aware routing protocol called MQ-Routing. But instead of proposing a new routing protocol, Hamrioui, et. al. [16], they exploited the existing AODV protocol by adding a new algorithm for energy fairness. The algorithm includes the clustering of nodes. Nodes with number of responsibilities are allowed more energy that other nodes in the network.

Compared to other papers, the papers [30][31][36] link the routing protocol to open issues in security. They proposed a modified

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

AODV [30] and Ad hoc On-demand Multipath Distance Vector (AOMDV) [36] routing protocol that uses RSA algorithm for authentication and blacklisting algorithm [31] to prevent the healthy nodes from sending data to the malicious nodes.

With all of the papers reviewed and analyzed, each of the papers did not specifically introduced problems in routing alone. Most of them provided trade-offs among other areas in which MANETs are challenged. The paper [3] is linked to topology controls, the papers [15] [16] are linked to energy usage and lastly, the papers [30][31][36] are linked to security.

3.3 Topology Control

The paper of Dhenakaran [3] stated that the mobility of the nodes in MANETs creates one of the most challenging topology issues. Several papers also indicate the same problem. The paper [44] links the topology control problem with performance. In the usual topology of MANETs, information is propagated through flooding. Kulkarni, et. al. [44] proposed a clustering scheme wherein clusters restrict the spreading of routing information only to cluster heads and gateway nodes. This avoids unnecessary wastage of resources such as bandwidth and energy.

Other topology control problems were stated in these papers [41][42]. The paper [41] stated that the interference among nodes and the limited network capacity [42] are among the other issues and challenges that MANETs face. [43][39] even implied a quality of service (QoS) requirement in terms of delay-constrained topology control problem. It is evident that MANETs have problems with regards to topology control. [41] proposed an interference-based topology control but the paper did not take delay requirement into consideration.

3.4 Energy

One of the important requirements of a MANET is energy efficiency. Energy efficiency increases the lifetime of the network. However, papers indicated different reasons for poor energy efficiency of some MANETs. One reason of the said problem is a not optimized clustering scheme [46]. The papers [45][44] even suggested a ways a node can harvest energy from the environment.

The paper [17] of Cyril and Zubair also stated that energy conservation is one of the most significant research areas in MANET due to the limited energy available to the nodes. Their paper proposed an algorithm for energy optimization called Distributed Energy Adaptation and Data Collection Algorithm (DEA-DCA).

Energy issues were also seen on MANETs used in military and rescue operations. The paper of Sandeep and Kumar [21] published the result of different cases where military scenarios are one of the highly sensitive MANET implementation needing energy efficiency solutions.

Similar to the papers in the of Routing, several papers [44][45][46] cut across different areas. This finding indicates that not enough number of MANET solutions address several areas at once.

4 CONCLUSION

The features of MANETs, together with the non-existence of a central base station, made MANET a very promising type of network. However, MANETs features also bring many new and existing issues and challenges in its implementation.

In this paper, several related literatures were reviewed to provide a summary of the existing issues and challenges in MANETs. All of the issues were categorized as follows: (1) security, (2) routing, (3) topology controls and (3)

energy efficiency. From the review of security issues and challenges presented by Dorri [5], several new issues were discovered, namely: New comer attack, Sybil attack, replay attacks, on-off attacks. However, several security issues still persist for example, black hole and malicious node attacks. This indicates that the solutions for these security issues were not very effective.

Several papers also did not specifically introduced problems in routing alone. A total of 6 papers were linked to other areas such as topology control, energy and security. This indicate that future solutions for MANET should also consider multiple or even all of the areas. The same observation is also noted in the area of energy, 3 papers say that the topology and routing have effect on every node's energy efficiency. Therefore, every area, in which MANETs are challenged, should be considered when proposing solutions.

5 REFERENCES

[1] M. &. G. S. (. Conti, Multihop ad hoc networking: The theory,
IEEE Communications Magazine.

[2] P. S. T. V. &. W. A. A. (. Patheja, An adaptive MAC 802.11
protocol for MANET using exponential algorithm., International Journal of Computer Science and Information Technologies, 4(2), 358-362.

[3] D. S. &. P. A. Dhenakaran, "An overview of routing protocols in
mobile ad-hoc network," International Journal of Advanced Research in Computer Science and Software Engineering, p. 2, 2013.

[4] M. &. G. S. Conti, "Mobile ad hoc networking: milestones,
challenges, and new research directions," IEEE Communications Magazine, pp. 52(1), 85-96, 2014.

[5] A. K. S. R. &. K. E. Dorri, "Security challenges in mobile ad hoc
networks: A survey," arXiv preprint arXiv:1503.03233, 2015.

[6] R. H. P. S. J. &. J. D. C. Jhaveri, "DoS attacks in mobile ad hoc
networks: A survey," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference, pp. 535-541, 2012.

[7] K. B. K. N. C. M. M. &. V. V. Villela, "A smart and reliable
crowdsourcing solution for emergency and crisis management," Interdisciplinary Information Management Talks, Podebrady, Czech Republic, pp. 213-220, 2014.

[8] S. S. N. R. M. &. A. M. H. Anjum, "Survey on MANET based
communication scenarios for search and rescue operations," IT Convergence and Security (ICITCS), 2015 5th International Conference, pp. 1-5, 2015.

[9] A. S. C. &. M. P. Goncalves, "Design of a mobile ad hoc network
communication app for disaster recovery," Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference, pp. 121-126, 2014.

[10] Q. T. N. K. &. Y. S. Minh, "DRANs: Resilient disaster recovery
access networks," Computer Software and Applications Conference
Workshops (COMPSACW), pp. 754-759, 2013.

[11] P. G. A. &. S. C. Morreale, "Mobile ad hoc network communication
for disaster recovery.," International Journal of Space-Based and Situated Computing, pp. 178-186, 2015.

[12] R. G. L. &. I. O. C. Narayanan, "A joint network for disaster
recovery and search and rescue operations," Computer Networks, pp. 3347-3348, 2012.

[13] Z. C. G. &. L. P. T. Lu, "Networking smartphones for disaster
recovery," In Pervasive Computing and Communications (PerCom),
2016 IEEE International Conference, pp. 1-9, 2016.

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

[14] H. &. C. N. Verma, "MANET based emergency communication
system for natural disasters," Computing, Communication & Automation (ICCCA), 2015 International Conference, pp. 480-485, 2015.
[15] D. O. G. &. P. A. Macone, "MQ-Routing: Mobility-, GPS-and
energy-aware routing protocol in MANETs for disaster relief scenarios," Ad Hoc Networks, pp. 861-878, 2013.
[16] S. L. P. L. J. &. L. M. Hamrioui, "Energy efficient in medical ad
hoc sensors network by exploiting routing protocols," Global
Communications Conference (GLOBECOM), pp. 2417-2422, 2014.
[17] O. C. &. R. A. M. J. Mathew, "A Novel Energy Optimization
Mechanism for Medical Data Transmission Using Honeycomb Routing," Journal of Medical Imaging and Health Informatics, pp. 857-862, 2016.
[18] P. J. &. H. K. L. Nicholas, "Computational challenges of dynamic
channel assignment for military MANET," Military
Communications Conference, MILCOM 2015-2015 IEEE, pp. 1150-
1157, 2015.
[19] R. M. R. &. C. J. H. Chen, "On modeling of adversary behavior and
defense for survivability of military manet applications," Military Communications Conference, MILCOM 2015-2015 IEEE, pp. 629- 634, 2015.
[20] M. P. B. K. &. P. B. Rath, "Energy efficient MANET protocol using
cross layer design for military applications," Defence Science Journal, pp. 146-150, 2016.
[21] J. &. K. J. S. Sandeep, "Efficient packet transmission and energy
optimization in military operation scenarios of MANET," Procedia Computer Science, pp. 400-407, 2015.
[22] X. Y. Z. Z. Z. C. D. &. P. F. Zhao, "Availability based trust model
of clusters for MANET," Service Systems and Service Management (ICSSSM), 2010.
[23] X. &. L. H. Lv, "Secure group communication with both
confidentiality and non-repudiation for mobile ad-hoc networks,"
IET Information Security, pp. 61-66, 2013.
[24] S. &. G. A. K. Sharma, "A Comprehensive Review of Security
Issues in Manets," International Journal of Computer Applications, p. 69, 2013.
[25] P. P. V. &. R. R. Goyal, "Manet: vulnerabilities, challenges, attacks,
application," IJCEM International Journal of Computational Engineering & Management, pp. 32-37, 2011.
[26] R. &. S. S. Jaiswal, "A novel approach for detecting and eliminating
cooperative black hole attack using advanced DRI table in Ad hoc Network," 2013 IEEE 3rd International, pp. 449-504, 2013.
[27] N. W. &. L. F. L. Lo, "A secure routing protocol to prevent
cooperative black hole attack in MANET," Intelligent technologies
and engineering systems, pp. 59-65, 2013.
[28] Z. A. &. I. M. H. Khan, "Wormhole attack: A new detection
technique," Emerging Technologies (ICET), pp. 1-6, 2012.
[29] M. S. S. D. R. A. &. K. P. Sathisha, "Implementation of Protected
Routing to Defend Byzantine Attacks for MANET's," International Journal of Advanced Research in Computer Science, p. 3, 2012.
[30] G. &. K. P. Singla, "A secure routing protocol for MANETs against
byzantine attacks," Computer Networks & Communications
(NetCom), pp. 571-578, 2013.
[31] M. Khari, "Mobile ad hoc netwoks security attacks and secured
routing protocols: A survey," International Conference on Computer Science and Information Technology, pp. 119-124, 2012.
[32] J. &. S. T. Soryal, "IEEE 802.11 Denial of Service attack detection

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

in MANET," Wireless Telecommunications Symposium (WTS), pp.
1-8, 2012.
[33] N. A. S. &. S. V. K. Dixit, "A Proposed Solution for security Issues
In MANETs," International Journal of Engineering Research &
Technology, p. 2, 2013.
[34] P. T. M. K. &. T. C. Tharani, "Secured consistent network for
coping up with gabrication attack in MANET," international journal of Emerging Technology and Advanced Engeineering, p. 3, 2013.
[35] G. &. B. S. Usha, "Impact of Gray hole attack on adhoc networks,"
Information Communication and Embedded Systems (ICICES), pp.
404-409, 2013.
[36] M. &. L. M. Salmanian, "Enabling secure and reliable policy-based
routing in MANETs," MILITARY COMMUNICATIONS CONFERENCE, pp. 1-7, 2013.
[37] P. &. K. P. Srinivasan, "REAQ-AODV: Route stability and energy
aware QoS routing in mobile Ad Hoc networks," Advanced

Computing (ICoAC), 2012 Fourth International Conference, pp. 1- 5, 2012.
[38] Q. Y. F. R. J. S. L. V. C. &. M. H. Guan, "Topology control in
mobile ad hoc networks with cooperative communications," IEEE Wireless Communications, p. 19, 2012.
[39] X. M. Z. Y. Y. F. &. V. A. V. Zhang, "Interference-based topology
control algorithm for delay-constrained mobile ad hoc networks,"
IEEE Transactions on Mobile Computing, pp. 742-754, 2015.
[40] H. N. T. A. N. &. K. N. Nishiyama, "On minimizing the impact of
mobility on topology control in mobile ad hoc networks," IEEE Transactions on Wireless Communications, pp. 1158-1166, 2012.
[41] L. H. R. Q. Q. Y. &. C. H. H. Zhou, "Energy-spectrum efficiency t
radeoff for video streaming over mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, pp. 981-991, 2013.
[42] K. Huang, "Spatial throughput of mobile ad hoc networks powered
by energy harvesting," IEEE Transactions on Information Theory, pp. 7597-7612, 2013.
[43] H. S. W. &. K. F. A. Ali, "Energy-efficient clustering in mobile ad-
hoc networks using multi-objective particle swarm optimization," Applied Soft Computing, pp. 1913-1928, 2013.
[44] S. B. &. Y. B. N. Kulkarni, "Challenges and Issues of Cluster Based
Security in MANET," IOSR Journal of Computer Engineering
(IOSR-JCE), pp. 1-5, 2016.
[45] R. &. K. D. Singh, "MANET: Security Issues and Behavior
Analysis of Routing Protocol Using NS-2," International Journal of Advanced Research in Computer Science and Software
Engineering, 2015.
[46] P. K. &. B. B. P. Krishnappa, " Investigating open issues in swarm
intelligence for mitigating security threats in MANET," International Journal of Electrical and Computer Engineering, 2015.
[47] S. C. M. G. S. &. S. I. (. Basagni, Mobile Ad Hoc networking: the
cutting edge directions (Vol. 35), John Wiley & Sons.
[48] S. C. M. G. S. &. S. I. (. (. Basagni, Mobile ad hoc networking, John
Wiley & Sons.
[49] F. R. T. H. B. S. &. Z. D. Yu, "Security and quality of service (QoS)
co-design in cooperative mobile ad hoc networks," EURASIP Journal on Wireless Communications and Networking, p. 188, 2013.
[50] A. El-Sayed, "Clustering based group key management for
MANET," Advances in Security of Information and Communication Networks, pp. 11-26, 2013.

Volume 2, Issue 1, 2017
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

[51] M. P. R. &. K. A. V. A. Achankunju, "Particle swarm optimization based secure QoS clustering for mobile ad hoc network," Communications and Signal Processing (ICCSP), pp. 315-320, 2013.

[52] J. S. M. K. A. &. R. M. M. Leiharungbam, "A SURVEY ON SECURITY ISSUES IN MANET: CHALLENGES, ATTACKS, AND SOLUTIONS," Asian Journal of Information Science and Technology (AJIST), pp. 7-11, 2016.

[53] S. P. S. &. S. G. Nithya, "Security Issues & Challenging Attributes in Mobile Ad-Hoc Networks (MANET)," 2016.

[54] M. H. A. A. &. I. M. Gharehkoolchian, "Improving security issues in MANET AODV routing protocol," International Conference on Ad Hoc Networks, pp. 237-250, 2015.

[55] M. &. R. U. P. Rath, "Analysis and Study of Security Aspect and Application Related Issues at the junction of MANET and IoT," International Journal of Research in Engineering and Technology (IJRET), pp. 4-7, 2015.