AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178
EISSN: 2309-8414

DOI: 10.22587/ajbas.2017.11.15.4
Journal home page: www.ajbasweb.com

Future Barriers, Challenging Security Attacks and Secure Routing Issues in MANET

[1]Ahmed K. Al-Shammari, [2]P Ehkan,[3]Naimah Yaakob

[1]Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
[2,3]Senior lecture, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.

Address For Correspondence:
Ahmed K. Al-Shammari, Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
E-mail: ahmedkareemhamzah@gmail.com

ARTICLE INFO

Article history:
Received 12 October 2017
Accepted 22 December 2017
Available online 31 December 2017

Keywords:
MANET; Security Attacks; Secure Routing Protocols.

ABSTRACT

Mobile Ad Hoc Network (MANET) was created as Packet Radio Network (PRNET) in 1970. More than four decades are elapsed to work on it. MANET is open nature scenario that is infrastructure less, in other words, it has no any fixed infrastructure to control and monitor, each node works likes a router. It has dynamic topology, therefore; MANET is easy to create for any task and for any type of network based on applications. It rely on wireless links therefore, wireless links are examined by different researchers and reported various type of security attacks. MANET is easy to be targeted due to open nature. Due to it, facing many issues while major issues like security issues, secure routing issues and so on. To mitigate these issues many researchers and industries have developed and proposed different kind of routing protocols and techniques to detect and prevent the security attacks, it is important to analyze the current development which will give the direction for further development. In this paper, we shall examine in detail different type of attacks that are considered as challenging security issues, secure routing protocols, observed challenges of MANET and finally discuss the open issues of MANET.

INTRODUCTION

There are two kinds of networks wired networks and wireless networks, MANET is a type of wireless network. MANET is an infrastructure less network (Moraes I.M., *et al*., 2016; Sesay, S.,*et al*., 2004). Which is a group of random self-organized nodes that can be deployed in any place and at any time. There is a mature condition after deployment that each node must communicate within the radio range, as well as the communication can be done by using multi-hop routing. Figure 1 shows the example of MANET. In figure 1, it elaborates the simplest view of a MANET. In this example there are three nodes namely; A, B and C. let suppose A wants to communicate with C while C is not in the range of A and far from each other thus B can use to forward packet between A and C, it is clear that B is within the range of A and C. Hence, B can act as a router.

It is cleared that each node act as a router and a host that enabling the forwarding of packets to the enabled node in the network when a route is recognized. due to open nature, MANET is vulnerable to different kind of attacks such as Blackhole, Grayhole, Dynamic denial of service, timing, Sybil, Sinkhole and wormhole attacks, furthermore, it is easy to eavesdropping due to dynamic network topology wireless and open nature (Jin, L., *et al*., 2006; Yerneni, R., *et al*., 2012). In general, security attacks are affected at breaking and spoiling the routing of control and data packets, in resultant, MANET becomes unsafe and useless. In Reactive routing protocols facing vulnerable to many attacks (Perkins, C., *et al*., 2003). The network damages mostly effected from Dynamic denial of service (dDoS) attack that is most simple due to its strong influence (Das, K., *et al*., 2014).

To Cite This Article: Ahmed K. Al-Shammari, P Ehkan, Naimah Yaakob, Future Barriers, Challenging Security Attacks and Secure Routing Issues in MANET. ***Aust. J. Basic & Appl. Sci.,*** *11(15): 20-25, 2017*

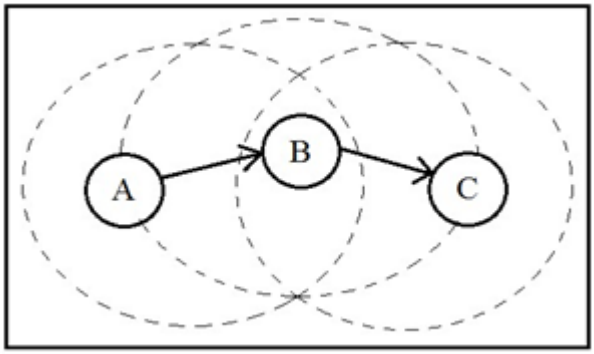

Fig. 1: example of Mobile Adhoc Network

MANET routing protocols are classified as proactive, reactive and Hybrid (Hinds, A., *et al*., 2013; Abusalah, L., *et al*., 2008; Abolhasan, M., *et al*., 2004; Zou, X., *et al*., 2002)[7-10], these routing protocols are depended on the process used for routes. While Attacker nodes target intentionally to interrupt the process of these routing protocols. For example, as denial of service can be done by attacker nodes. Malicious nodes try to handle or alter accurate routing information to achieve their target either in the active or passive way. In this paper, we shall focus on major security attacks and secure routing protocols in MANET. We discussed overall observed challenges of MANET and highlighted open research issues in this paper that can be helpful for researchers to understand the research scope of network security and help to create some possible solutions to mitigate these challenges and finally conclude to findings in conclusion section.

Attacks in MANET:

As long as development of multiple applications to facilitate reliable usage of MANET and accurate communication brings many challenges, security attacks are one of the most potential issues in MANET. Many authors have proposed solutions and highlighted security attacks in MANET (Alani, M.M., 2014; Sharma, K., *et al*., 2010; Chen, J., *et al*., 2007). MANET security attacks are the biggest barrier for further development and activation of applications. The serious challenging attacks are described in the following subsections.

Eavesdropping Attacks:

Eavesdropping is due to open nature; therefore, outsiders can grab the information during forwarding packets (Liang, Y., *et al*., 2011). It is an exclusive procedure of an attacker node is enabled during transmission, in general, these kind of attacker nodes listen to the messages by an unplanned receiver node (Florian, D., 2008). Appropriate tuning up the receiver node to a particular frequency interrupts wireless medium. The main purpose of this attack to steal some useful information that can be used to harm particular node or group of nodes, normally it an unauthorized node attempts to capture the private key, public key etc. This kind of attack generally executes by tapping the wireless links. Once the information is captured then possibly it can be used to harm any particular node.

Jamming Attacks:

Jamming attacker node is particular to wireless medium instead of the wired network because there is no conception of signal jamming. In a wireless network, this attack only targets the network performance which dramatically degrades the routine and normal performance of the network by dropping the signal accessibility (Lazos, L., *et al*., 2009; Xu, W., *et al*., 2005). A node represents itself as an adversary, which is identified as a jammer, furthermore, produces the radio signals to rush up partly or even fill-up entirely the wireless band. In resultant, the plenty of adverse the signals, the authentic nodes and entire traffic can be jammed by this kind of attack (Xu, W., *et al*., 2004). It is easy to generate a jamming attack, initially the frequencies of the authentic signal of the network is verified and then the jamming attackers are generated by jammer node. Typically, jammers block the authentic traffic by using flooding and then filling up the accessible band.

Denial of service (DoS) Attacks:

DoS attackers nodes are very harmful to entire network which focused on taking the availability of the network or nodes or any services which are activated and controlled by any particular network or service. It can be said that this kind of attack triggered the unavailability from the availability of any network or nodes or services to the particular receiver. DoS entered into the network in shape of a malicious that is a compromised node in the network. DoS can be triggered in any shape such as looking on entire network or node or services. Having the advantage of weaknesses of Link Layer an attacker node can be utilized the binary exponential scheme of IEEE802.11 to denial entree to its native neighbors (Alani, M.M., 2014; Sharma, K., *et al*., 2012).

DoS attacker node can be targeted a authenticate node for concentrated fake routing to use its power resource. In resultant, a node may change its activation into sleep state and disruption collaborative algorithms. This kind of Attacker node also applies the jamming attacker procedure to execute the DoS attack. Flooding the network by the adverse signal can be blocked the authentic network (Xu, W., *et al*., 2014).

Blackhole Attacks:

In a Blackhole, the routing attack a malicious enable a false and promotes as an ideal alternative for routing to destination from a particular source by itself (Padilla, E.G., *et al*., 2007; Bar, R.K., *et al*., 2013)[19-20]. In this kind of attack, once received a route request the adversary node quickly retorts with a false straight path to the destination from a particular source (Gideon, N., *et al*., 2014). To receive the false route retorts the source node forward the packet through adversary node. In resultant, to achieve routing opportunity as a midway node can be done any modification in genuine packet earlier additional forward to next hop.

Rushing Attacks:

The rushing attack is introduced in (Yi, S., *et al*., 2001) as a new routing attack. there are many routing protocols but on-demand routing protocol is vulnerable to rushing attack. In this attack, the routing discovery is disrupted by enabling duplicate routes to overthrow in establishing of routing discovery (Yi, S., *et al*., 2001; Saini, A. and H. Kumar, 2010). Flooding is considered a serious problem in on-demand protocols due to this DSR and AODV keep a method to get over flooding. Furthermore to get over on flooding, node forward only individuals requests that are arrived first. Rushing attack holds the benefit of this weakness.

Wormhole Attacks:

In wormhole attacker node, the nodes more than one malicious node to be compared with rushing attack, in rushing attack there is a duplicate. In wormhole attacker node, a malicious node gets a packet, it transmits to another malicious node via a channel, which controls channel among malicious nodes is known as wormhole attack (Sadeghi, M. and S. Yahya, 2012). A participant pretends as attacker node which enables the wormhole to receive entire network's nodes by generating an impression of the finest vacant path to the source node. The whole process is gone via channel (Li, W. and A. Joshi, 2008; Jawandhiya, P.M., *et al*., 2010). Due to its attractive appearance, it grabs all traffic and interrupts the routing protocols by representing itself as a trustworthy route.

Sinkhole Attacks

MANET is facing a serious threat from Sinkhole attack (Chen, J., *et al*., 2007). MANET have plenty of routing protocols and open nature due to this a malicious node transmit the wrong routing to grab all traffic towards by showing itself an authentic and having shortest path toward the destination. Due to these kind of nature of Sinkhole, the whole traffic diverts all traffic to itself and after getting all traffic attention it can be changed the information or modify the information before sending to the destination or can be easily dropped that packet without sending to the destination. Sinkhole node attempts to capture the information of coming packets and then utilized that secure information against any purpose. On the other hand, Sinkhole node can be effected the whole performance or routing as well as a network such as routing protocol AODV by maximize the order number or minimize the hop count (Chirala, A.P., 2010; Radosavac, S., *et al*., 2004). Due to this, a Sinkhole node can be claimed to having the reliable vacant path which is gone through it.

Sybil Attacks:

The stolen or fabricated node inside the network claims fake identification or showing fake identification is called Sybil attack which are normally in the number of the same node in multiple numbers or same node in multiple identifications in a network by creating multiple fake nodes in a network. In resultant, a particular node shows itself as multiple individuals and authentic nodes in a network (Chen, J., *et al*., 2007). These multiple nodes having fake identification can harm and misguide the entire network, such as voting, billing, credit cards, access control etc. are a serious and challenging issue to detect the Sybil node (Haifeng, Yu., *et al*., 2008; Kim, K. and S. Kim, 2007). Due to generated multiple fake nodes in the network, it is hard to detect the malicious node, on the other hand, Sybil nodes can be jam whole network and degrade the network performance by creating huge traffic. This kind of issues leads the network by facing multiple issues such as unfair resource allocation, denial of service etc. there are many possible ways to detect Sybil attack but due to less power of nodes and infrastructure less network makes harder to detect Sybil attack in MANET.

Byzantine Attacks:

As it is known that a malicious node or hacker node work with some groups or use multiple resources, same as Byzantine node is involved in a group of malicious nodes in a network or it may be a single node. Commonly

Byzantine node objective to harm the MANET by generating routing loops to damage overall routing assistances of the network (Crepeau, C., *et al*., 2007).

Session Hijacking Attacks:

MANET is providing just primary operation of the session. While it is not providing a suitable session security procedure throughout the communication between nodes in the network. Malicious node uses the benefit of this weakness to the attacker node to act as an authentic node for generating the Section Hijacking (Sharma, K., *et al*., 2010; Chen, J., *et al*., 2007).

Routing in MANET:

At the moment, in MANET various novel routing protocols introduced by researchers to facilitate MANET applications (Hinds, A., *et al*., 2013; Zou, X., *et al*., 2002). Due to limited battery power and range, frequently topology change and scalability introduce many challenges to overcome these limitations in Routing of MANET. Furthermore, Size of routing table disturbs the link overhead. Recently, it is observed that to reduce these limitation, researchers are putting their efforts to design effective and trustworthy routing protocols. Figure 2 shows the three type of routing protocols of MANET and it can see that hybrid routing protocol is a combination of proactive and reactive routing protocol.

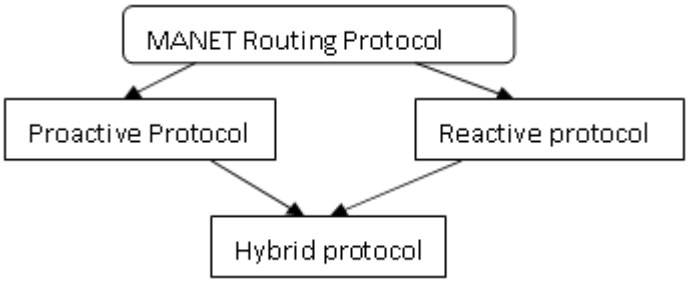

Fig. 2: MANET Routing Protocols

Proactive Routing Protocol:

Proactive routing is also called table-driven routing (Abusalah, L., *et al*., 2008; Abolhasan, M., *et al*., 2004). Normally, it keeps one or more routing tables for storing the routing information. Furthermore, change in the information of the topology can be propagated to all packets. Proactive routing used to maintain an effective route for packets delivery. Due to the monitoring of route discovery of routing table for each node actively accessible. Proactive routing has a different procedure to update the table of routing. There are a different kind of proactive routing protocols such as Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) Optimized Link State Routing Protocol (OLSR) and Fisheye State Routing (FSR) etc. are considered as most reliable and useable routing protocols due to their satisfied performance (Zou, X., *et al*., 2002).

Reactive Routing Protocol:

Reactive routing is also called on demand routing (Zou, X., *et al*., 2002). Normally, it is a procedure which is using for discover the route. Due to discovering the routes, it helps to minimize the network traffic load, which is the main aim of the reactive routing protocol. As proactive routing is responsible for maintaining the routing table while reactive routing has no need to maintain routing table it simply discovers the route discovery. In other words, it can define that if any node wants to forward the packet from source to destination, at the initial step it gone through to the discovery of finding the best route towards the destination. Proactive routing also maintains its cache to store to routes and when it needed it provide to requested route. Proactive routing uses more bandwidth of the network while reactive uses less. Well known proactive routing protocols like Dynamic Source Routing (DSR) and Adhoc On-Demand Distance Vector routing (AODV) mostly reliable and promoted from many researchers (Gokhale, V., *et al*., 2010; Amitabh, M., 2008).

Hybrid Routing Protocol:

Proactive and reactive routing protocols are optimal useable when the number of nodes are less or light network having less traffic. While when the network traffic increase in the number of nodes proactive and reactive protocols are not reliable. Therefore, to satisfy and provide good quality of the network in term of dealing with a huge number of nodes it required the hybrid routing protocol. Normally, hybrid routing is a concept of a combination of proactive and reactive routing protocols which uses the features of proactive and reactive routing protocols. Hybrid routing protocol using the number of groups and clusters, which is suitable

for a huge number of nodes in the network. On the other hand, these routing protocols have the disadvantage to utilizing more power as well as memory for routing. Zone Routing Protocol (ZRP), Hazy Sighted Link State (HSLS) protocol and Secure Routing Protocol (SRP) are known hybrid routing protocols (Gokhale, V., *et al*., 2010; Amitabh, M., 2008).

Observed Challenges of MANET:

MANET is the network of the era and facilitates as wireless in nature and collaborator as a communication medium between one or many nodes. In this article is discussed major vulnerabilities of MANET in detail. In a broad view, due to these vulnerabilities of the MANET and secure routing protocols are needed to take a serious concentration to reduce major issues. The researchers have done a lot of research work while still, these barriers bring a week picture and instability in the term to satisfy security issues which are discussed in above sections; furthermore, scalability of secure routing protocols is challenging issue. We have observed that until now there is needed to relook these issues especially can be found a great research scope in the area of security of MANET. On the other hand, secure routing protocols are the essential for secure communication in the MANET thus secure routing protocols can be high valued and can be targeted by the malicious nodes as well as attackers. There are a lot of security attacks have been discussed by researchers and the most of the major attacks are discussed in above section. These security attacks are mostly considered as routing attacks in MANET obtain the benefit of the various weaknesses of the secure routing protocols. Thus, the design of new secure routing protocols are challenging research area for the developers and considered as a major issue in MANET. There are a lot of techniques are proposed and designed for detecting attacks while most of the techniques have some major or minor limitations furthermore, some of the proposed techniques are designed and proposed only for specific attack and a specific protocol. In resultant, the proposed techniques cannot fulfill the security requirements or not effective in the presence of various security attacks. We have observed that until now there is no proposed solution to design a standard attacks detection and prevention technique that should deal with the multi range of the security attacks in MANET, this can be considered as an open research issue.

Conclusion:

Major security attacks and routing protocols are discussed in this paper that will helpful and useful for researchers to categorize major challenges. Most of the new routing protocols have proposed by different researchers while until now open challenges degrade the network performance. Due to not considering security at the main priority in routing protocols such as routing protocols should deal with all kind of attack detection and prevention by itself while until now hard to find that kind of secure routing protocols. It is clearly open research issue to design a secure protocol which should deal all kind of attacks. We highlighted secure routing protocols and security challenges barriers of the MANET that should take a serious note to relook their solutions. MANET is an open source network which is facing many problems major security attacks have discussed in this paper, Wireless network is pretty smarter than wired network but security is an active open research issue, day by day many new security challenges are perceiving. Therefore, the significant development is mandatory to enable MANET smarter and most secure.

REFERENCES

Abolhasan, M., T. Wysocki and E. Dutkiewicz, 2004. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, (2): 1–22.

Abusalah, L., A. Khokhar and M. Guizani, 2008. “A Survey of Secure Mobile Ad Hoc Routing Protocols” IEEE Communications Surveys & Tutorials, 10(4).

Alani, M.M., 2014. “MANET Security: A Survey” IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, pp: 28-30.

Amitabh, M., 2008. “Security and Quality of Service in Ad Hoc Wireless Networks”. Cambridge University Press, Cambridge.

Bar, R.K., J.K. Mandal and M.M. Singh, 2013. "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack," in Proceedings of International Conference on Computational Intelligence: Modeling Techniques and Applications.

Chen, J., J. Wu, M.C.B. Wu, 2007. "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless Network Security, Yang Xiao, XueminSherman Shen, and Ding-Zhu Du, Eds. USA: Springer US, 2007.

Chirala, A.P., 2010. “Analysis and Diminution of Security Attacks on Mobile Ad Hoc Network”. IJCA Special Issue on “Mobile Ad-Hoc Networks”, MANETs, pp: 105-110.

Crepeau, C., C.R. Davis and M. Maheswaran, 2007. "A Secure MANET Routing Protocol with Resilience against Byzantine Behaviours of Malicious or Selfish Nodes," in 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07.

Das, K. and A. Taggu, 2014. "A comprehensive analysis of DoS attacks in Mobile Adhoc Networks." In proceeding of International Conference on Advances in Computing, Communications and Informatics, pp: 2273-2278.

Florian, D., 2008. "Security Concepts for Robust and Highly Mobile Ad-hoc Networks".

Gideon, N. and B.K. Edwin, 2014. "Clustering Effects on Wireless Mobile Ad-Hoc Networks Performances", in International Journal of Computer Science & Information Technology (IJCSIT), 6: 1-19.

Gokhale, V., S. Ghosh and A. Gupta, 2010. "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks: A Survey". In: Pathan, A.S.K., Ed., Security of Self-Organizing Networks, MANET, WSN, WMN, VANET, Auerbach Publications, Boston, pp: 195-225.

Haifeng, Yu., P.B. Gibbons, M. Kaminsky and Feng Xiao, 2008. "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks," in IEEE Symposium on Security and Privacy (SP 2008).

Hinds, A., M. Ngulube, S. Zhu, and H. Al-Aqrabi, 2013. "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)" International Journal of Information and Education Technology, Vol. 3(1).

Jawandhiya, P.M., M.M. Ghonge, M.S. Ali and J.S. Deshpande, 2010. "A Survey of Mobile Ad Hoc Network Attacks". International Journal of Engineering Science and Technology, 2: 4063-4071.

Jin, L., Z. Zhang, D. Lai and H. Zhou, 2006. "Implementing and evaluating an adaptive secure routing protocol for mobile ad hoc network." In Wireless Telecommunications Symposium, pp: 1-10.

Kim, K. and S. Kim, 2007. "A Sinkhole Detection Method Based on Incremental Learning in Wireless Ad Hoc Networks".

Lazos, L., S. Liu and M. Krunz, 2009. "Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks" in Proceedings of the Second ACM Conference on Wireless Network Security, Zurich.

Li, W. and A. Joshi, 2008. "Security Issues in Mobile Ad Hoc Networks—A Survey". Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, pp: 1-23.

Liang, Y., H.V. Poor and L. Ying, 2011. "Secrecy Throughput of MANETs Under Passive and Active Attacks," IEEE TRANSACTIONS ON INFORMATION THEORY, 57(10): 6692-7002.

Moraes I.M., M.G., M.E.M. Campista, L.H.M.K. Costa, O.C.M.B. Duarte, 2006. "A Survey on Wireless Ad Hoc Networks", In: Pujolle G. (eds) Mobile and Wireless Communication Networks. IFIP The International Federation for Information Processing, vol 211. Springer, Boston.

Padilla, E.G., N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, 2007. "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs," in 32nd IEEE Conference on Local Computer Networks (LCN 2007), Dublin.

Perkins, C., E. Belding Royer and Samir Das, 2003. "Ad hoc on-demand distance vector (AODV) routing,". IETF, RFC 3561, July 2003. http://www. 1eft.

Radosavac, S., N. Benammar and J.S. Baras, 2004. "Cross-Layer Attacks in Wireless Ad Hoc Networks". Proceedings of the 2004 Conference on Information Sciences and Systems, Princeton, pp: 17-19.

Sadeghi, M. and S. Yahya, 2012. "Analysis of Wormhole attack on MANETs using different MANET routing protocols," in Fourth International Conference on Ubiquitous and Future Networks (ICUFN), Phuket.

Saini, A. and H. Kumar, 2010. "Effect of Black Hole Attack on AODV Routing Protocol in MANET". International Journal of Information Technology, Modeling and Computing (IJITMC), 2: 9-17.

Sesay, S., Z. Yang and J. He, 2004. "A Survey on Mobile Ad Hoc Wireless Network" Information Technology Journal, 3(2): 168-175.

Sharma, K., N. Khandelwal and M. Prabhakar, 2010. "An Overview Of security Problems in MANET," in Proceedings of the International Conference on Network Protocols (ICNP), Kyoto.

Xu, W., T. Wood, W. Trappe and Y. Zhang, 2004. "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service". In Proceedings of the 3rd ACM Workshop on Wireless Security, ACM Press, New York, pp: 80-89.

Xu, W., W. Trappe, Y. Zhang and T. Wood, 2005. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks". In Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM Press, New York, pp: 46-57.

Yerneni, R. and A.K. Sarje, 2012. "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc." In Proceeding of Third International Conference on Computing Communication & Networking Technologies (ICCCNT), pp: 1-5.

Yi, S., P. Naldurg and R. Kravets, 2001. "Security-Aware Ad Hoc Routing for Wireless Networks", In: Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, ACM Press, New York, pp: 299-302.

Zou, X., B. Ramamurthy and S. Magliveras, 2002. Routing techniques in wireless ad hoc networks classification and comparison. In proceedings of the Sixth World Multiconference on Systemics, Cybernetics, and Informatics (SCI 2002), Florida, US, July 14–18, 2002, volume 4.