International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 1833-1841
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A STUDY ON DIFFERENT SECURITY ATTACKS ASSOCIATED WITH ROUTING IN MOBILE AD HOC NETWORKS

Lakshman Naik.L[1], R.U.Khan[2], R.B.Mishra[3]
[1, 2]Department of ECE, BHU, Varanasi, India
[3]Department of CSE, BHU, Varanasi, India

ABSTRACT: Wireless networks which operate without the need of central gateways and by employing multi-hop radio transmissions are called mobile ad hoc networks (MANETs). They gain dynamic topologies because of their node mobility in random directions. Due to unavailability of fixed infrastructure (such as central network gateways, wireless access points etc.), MANETs are highly vulnerable to security attacks. Routing protocols in mobile ad hoc networks discover routes between communicating nodes. Moving nodes pose several challenges for routing protocols in these networks. Mobile ad hoc networks has some exclusive characteristics such as; physical vulnerability, dynamic network topology, inadequate availability of resources (such as battery power and the bandwidth), shared radio channels, lack of central infrastructure, lack of association among network nodes and uncertain operating environments. These characteristics put MANETs vulnerable to high security risks. Over the years, many security solutions have been provided for mobile ad hoc networks but still they need enormous, full proof and easy security solutions. There are numerous routing protocols available for mobile ad hoc networks. Most of the proposed security solutions are limited to few well-known routing protocols. This paper sketches security attacks associated with the routing in mobile ad hoc networks and presently available solutions in detail. This may help researchers in addressing security solutions for other routing protocols available for the mobile ad hoc networks.

Keywords: MANETs, Routing, DoS, Security, Solution.

INTRODUCTION

Mobile ad hoc networks often referred as MANETs are new generation wireless networks; the principal behind these networks is multi-hop relaying. MANETs operate without requiring any fixed infrastructure such as; base stations, central network gateways and wireless access points. Nodes of MANETs are mobile in nature; they act as host and the router. Mobility of nodes in random directions cause mobile ad hoc network to obtain dynamic network topologies [1, 2]. Routing protocols initiate route discovery between source and the destination nodes. Dynamic network topologies dispense many challenges over the routing protocols while establishing an efficient and error free communication path between network nodes. In MANETs, security threats mostly occur on the network layer over an established communication link. This is due to some of MANET's own characteristics such as; physical vulnerability, dynamic network topology, inadequate availability of resources such as battery power and the bandwidth, shared radio channels, lack of central infrastructure, lack of association among network nodes and uncertain operating environments. In order to overcome from the possible security attacks, a security aware routing protocol must address some basic security requirements like; non-repudiation, network availability, integrity and confidentiality. Security attacks in mobile ad hoc networks are classified broadly as active and passive attacks [1].

Active attacks can destroy or revise the live network and routing data causing malfunctioning of the network. Passive attacks are dangerous as they does not disturb network operation but they snoops network data without any changes. Different types attacks in MANETs can be classified as; network layer attacks, transport layer attacks and application layer attacks. Attacks pertaining to the network layer are; wormhole attack, resource consumption attack, blackhole attack, information disclosure and byzantine attack etc. Session hijacking is specific type of attack associated with the transport layer and the repudiation attack is generally occurs over the application layer. Other attacks associated with the MANETs are; multi-layer attacks and device tampering. Denials of service (DoS) and impersonation attacks are associated with the multi-layer attacks. Jamming, SYN flooding and distributed DOS (DDoS) attacks are multi-layer denial of service

attacks generally referred as DoS attacks. Fig.1 shows the classification of security attacks in MANETs [1, 2].

Routing protocols in MANETs face several routing attacks which targets disruption of the network operation. Some of them include; rushing attack, packet replication, route cache poisoning, route table poisoning and routing table overflow. These routing attacks falls under network layer attacks in mobile ad hoc networks. In order to prevent the routing attacks, a secure routing protocol is needed for better operation of the network. In MANETs, nodes have to perform as a host (source or destination) as well as router due to absence of centrally controllable -network infrastructure. Thus, unavailability of dedicated routers poses several challenges in providing secure and error-free routing [1, 2]. Routing protocols in MANETs get affected by different ways of security attacks which disorders routing processes by altering established communication paths and by intruding invalid data packets along the path [3]. Other reasons which make secure communication difficult are; random mobility of network nodes, limited obtainability of resources (bandwidth, memory and battery power) limited processing power. Therefore, a secure routing protocol require some basic requirements such as stability against routing attacks, correct path discovery guarantee, finding of malicious nodes and privacy of network topology. Some of the security aware routing protocols proposed for MANETs were; SA-AODV (Security Aware – Ad hoc On demand Distance Vector), SAR (Security aware Ad hoc Routing), ARAN (Authenticated Routing for Ad hoc Networks) and SEAD (Secure Efficient Ad hoc Distance vector) etc. Recent researches have proposed their new versions.

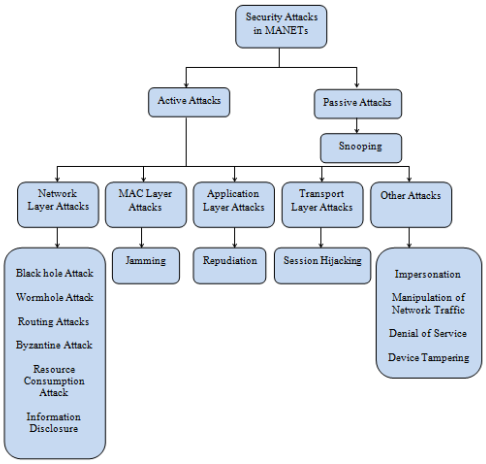

Figure 1. Classification of Security Attacks in MANETs

Still there is large scope in addressing security challenges faced by the MANET routing protocols in order to ensure secure and safe operation of mobile ad hoc networks [1, 3].

1. NETWORK LAYER ATTACKS IN MANETS

Some well-known security attacks in mobile ad hoc networks are; information disclosure attack, resource consumption, byzantine, blackhole, wormhole and routing attacks.

1.1 IDA (Information Disclosure Attack)

This attack involves compromising of a MANET node. By this attack, a compromised node can disclose confidential and important network information such as; available optimal paths, network topology and geographical locations of the network nodes etc., to the unauthorized nodes involve in the network communication [1, 2].

1.2 RC (Resource Consumption)

This attack involves with consumption of resources such as; computational power, battery power and the bandwidth available with the network nodes. By this attack, a malicious node in the network tries to waste key resources available with the authorized network nodes [1, 24].

1.3 Byzantine

Byzantine attacks are generally performed by the malicious intermediate nodes in the network. Any single or group of comprised intermediate nodes involves performing this attack. By this attack, malicious intermediate nodes create routing loops, drop the data packets and establish communication over non-optimal routes. MANETs attacked by byzantine attacks would appear functioning normally in order, but they show byzantine activities [1, 4].

1.4 Blackhole

In blackhole attacked MANETs, malicious nodes wrongly announce shortest routes as most stable routes between source and the destination nodes. Such route announcements occur during path finding process causing wrong route entries in the routing tables available with the network nodes. Thus, malicious nodes attacked by the blackhole attack divert some or

all the data packets to false routes other than the valid route the destination node [1, 20].

1.5 Wormhole

In wormhole attack, an attacker creates tunnel between two locations within the network and transfer received packets through the tunnel. It results in resending up of packets in to the network. Tunnel formed between two conspiring locations termed as a wormhole. An attacker misuse broadcast nature of the radio channels for creating wormholes for those data packets which are not addressed to them. After creating a wormhole, an attacker gains some sort of control over the network. This prompts other nodes compromised to network security. Proper solutions are required to protect MANETs from wormhole attacks. Due to Wormhole attacks in MANETs, most of the existing routing protocols face difficulties in discovering valid paths to the destinations [1, 5, 24].

1.6 RA (Routing Attacks)

Routing attacks referred to many attacks throw upon the MANET routing protocol which targets distraction of network operations.

2. ROUTING ATTACKS IN MANETS

Routing is the process by which network nodes discover valid paths between them for error free and efficient communication as and when required. An attacker usually targets routing protocols to disturb valid route discovery which in turn, disrupt entire network operation. Different attacks faced by the MANET routing protocols are; rushing attack, routing table overflow, route cache poisoning, routing table poisoning and packet replication etc.

2.1 Rushing

During path finding process, most of the on-demand MANET routing protocols use duplicate suppression. This makes them vulnerable to rushing attack. Upon receiving a RREQ (Route Request) packet from the source node, an adversary node floods the RREQ packets quickly throughout the network before any other network node (which also receive the same RREQ) react. All other nodes receive RREQ packet sent by the adversary node and discard the original RREQ packets sent by the source node by duplicate suppression. Thus, source node gets false routes which include adversary node as an intermediate node. Detecting rushing attack in MANETs is a difficult task [1, 6, 24].

2.2 RT (Routing Table) Overflow

As compared to reactive MANET routing protocols, proactive MANET routing protocols are more vulnerable to this attack. This attack causes an overflow of routing tables which results in no new route entries in the routing tables available with the authorized nodes. In this attack, an adversary node broadcast path information to unauthorized as well as authorized nodes of the network. This causes an overflow of routing tables in the network [1, 24].

2.3 RC (Route Cache) Poisoning

In this type of attack, an adversary node poison the route cache in the similar manner on-demand MANET routing protocols maintains a route cache. Route or path cache holds latest information pertaining to valid routes [1, 24].

2.4 RT Poisoning

In this attack, compromised nodes broadcast false routing updates to authorized nodes which results in improper routing in the network. Further it causes the whole or part of the network unapproachable [1, 24].

2.5 PR (Packet Replication)

This type of attack creates misperception in the routing process. Here, a compromised network node replicates stale data packets throughout the network. This causes consumption of extra battery power and bandwidth (resources) available with the network nodes [1, 24].

3. PREREQUISITES OF SECURE ROUTING

A security aware MANET routing protocol must meet some basic requirements such as; stability, correct path discovery guarantee, discovery of malicious nodes and secrecy of network topology [1, 2, 3].

3.1 Stability

MANET routing protocols must have stability to regress their operation in case any security attack. They must pay attention to get rid of attacks and maintain normal routing processes [1, 2].

3.2 Correct Path Discovery Guarantee

A MANET routing protocol must able to find correct and guaranteed paths between source and the destination nodes. They must ensure availability of correct and error-free paths before processing a route request (RREQ) message [1].

3.3 Discovery of Malicious nodes

A security aware MANET routing protocol must have abilities to discover occurrence of malicious nodes in the network. They must elude involvement of such nodes in routing processes [1, 3].

3.4 Secrecy of Network Topology

Secrecy of network topology is an essential requirementof security-aware routing protocols because, disclosure of topological information leads to several attacks in the network. A malicious node can fetch topological information of the network by information disclosure attack. After knowing network topology, an attacker can easily study traffic patterns of the network and target most active nodes [1].

3.5 Security Aim

In order to achieve desired security aims, an ideal security aware MANET routing protocol must ensure certain pre-requisites such as; service availability, information confidentiality, secure data transmission, node authentication, anonymity, non-repudiation, co-operation among network nodes [2].

4. Some Earlier Security Solutions

Earlier, various solutions have been proposed for secure routing against attacks. Some of them are; SAR (Security Aware Ad hoc Routing), SEAD (Secure Efficient Ad hoc Distance vector), ARAN (Authenticated Routing for Ad hoc Networks) and SA-AODV (Security Aware-Ad hoc On-demand Distance Vector) etc.

4.1 SAR

Security aware ad hoc routing is one of the security aware routing protocols proposed for MANETs [2]. During path discovery, SAR considers security as one of its main metrics. SAR uses a frame work to enforce and measure various security metrics. This frame work provides different kind of security to various applications [1, 2, 7]. In MANETs, a source and the destination node communicate with each other through the intermediate nodes having some kind of trust over intermediate nodes. SAR routing protocol maintains certain kind of trust level while performing routing. It provides secured routing using trust level as one of the metric while routing. Fig. 2 explores trust levels in security aware ad hoc routing protocol.

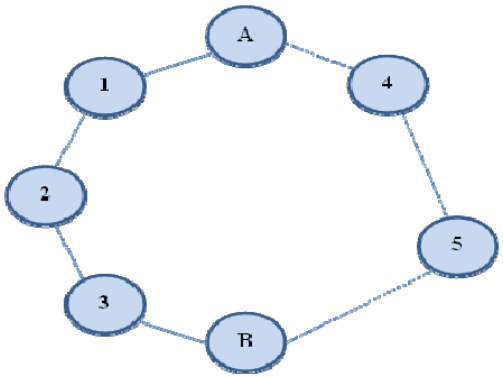

Figure 2. Trust levels in SAR

While selecting the routes, the SAR routing protocol operates on pre-defined trust levels. In Fig. 2, the node A intends to communicate with node B. There are two available routes between node A and B; A-1-2-3-B and A-4-5-B. Here, nodes 1, 2 and 3 are trusted intermediate nodes whereas nodes 4 and 5 are private intermediate nodes. Shortest route between node A and B is A-4-5-B which consists of private intermediate nodes. In this case, the SAR will select the long route A-1-2-3-B because it has trustable intermediate nodes. SAR uses security attentive packet forwarding mechanism which is embedded with different security levels.

Each and every data packet gets a security code before they leave. Intermediate network nodes also allied with certain security level. Upon receiving a data packet, the intermediate or neighbor node verifies its security level. If the security level of the received packet is less than that of the packet, the intermediate node will discard the packet [1, 2, 7]. SAR mechanism can certainly be integrated with any routing protocol available for MANETs. SAR permits applications to select their requisite security level which causes increased usage of security keys.

4.2 SEAD

SEAD is a security-aware routing protocol developed for mobile ad hoc networks. It works with the help of one way hash function and it does not support cryptography. SEAD is a DSDV (Destination Sequenced Distance Vector) based routing protocol specially designed to address resource consumption and denials of service (DoS) attacks. Secure efficient ad hoc distance vector (SEAD) basically works like standard DSDV routing protocol with upgradation of one way hash function. SEAD segregates updates received from

malicious and non-malicious nodes by the help of an authentication system which is based on one way hash function. SEAD eludes routing loops excepting the routing loops with multiple attackers. SEAD is a robust routing protocol for healing un-coordinated attacks. If an attacker uses matching sequence number and the metric of recently updated message to send a fresh routing update, then the SEAD would not overcome from such attacks [1, 2, 8, 24].

4.3 ARAN

ARAN is also a security aware routing protocol proposed for MANETs. It uses cryptographic certificates to defeat network layer attacks. ARAN requires prior security coordination among all the network nodes, it upkeeps non-repudiation, authentication and message integrity. In ARAN, upon receiving a RREQ, the destination node generates a RREP (Route Reply) message and unicast back it to the source node. In ARAN, establishment of secure path take place by two processes namely, preliminary cryptographic certification process and end to end route authentication process [1, 2, 3, 9].

4.4 SA-AODV

Security aware AODV routing scheme was designed to defeat a specific security attack by a single attacker. It is basically the standard AODV routing protocol with an enhanced feature to address a particular blackhole attack. SA-AODV totally eradicates an individual blackhole attack. This protocol despondently fails if the attacks were initiated by a group of malicious nodes. The foremost drawback of SA-AODV is significantly increasing control overheads [1, 3, 10, 11, 12].

4.5 ARIADNE

Researchers Yih-Chun Hu and Adrian Perrig were presented the ARIADNE secure routing model for the mobile ad hoc networks in the year 2005. Ariadne prevents DoS attacks and attacks that alter secure routes comprised of secure network nodes. It uses extremely effective symmetric cryptographic primitives. Ariadne is one of the efficient secure reactive routing protocols proposed for MANETs [21]. ARIADNE uses digital signature to validate network nodes. It works in two stages; in first stage, it verifies the route authenticity and in the second stage, it verifies any missing nodes falls on the hop count of RREQ (Route Request) or RERR (Route Error) messages. In ARIADNE, source node specifies media access control code along with a shared key [3, 24].

4.6 TAODV

TAODV (Trusted AODV) is also a proposed secure routing solution for MANETs. It provides security solutions to the standard AODV routing model by trust based mechanism. The TAODV builds a trust based relationship among all network nodes and promote trusted routing in the network. The TAODV easily spots the nodes which exhibit self-centric characteristics and carry mischievous behaviour. Network services to such mischievous nodes are discarded. This routing model has four modules namely, basic routing, trust model, trusted routing model and self-organized management model [2].

5. SOME RECENT SECURITY SOLUTIONS

Over the years, many new solutions were proposed to address routing attacks in MANETs. Some recent solutions were discussed here.

Researchers Sajal Sarkar and Raja Datta were worked on stochastic multipath routing and proposed a minimax-Q learning based security system which prevents adaptive security attack over an established communication link [13]. Researchers Shahjahan Ali, Prof. Parma Nand and Prof. Shailesh Tiwari were proposed a secure message broadcasting technique using cryptography for VANETs (Vehicular Ad hoc Networks, a special kind of MANETs). This technique addresses wormhole attacks in MANETs [14]. Researchers Priyanka Yadav and Muzzammil Hussain have proposed a secure AODV routing protocol using node authentication techniques. They introduced a mechanism of embedding digital certificate in HELLO packet for preventing unauthorized entries during a routing session [3].

Researchers Pawan Kumar Sharma and Vishnu Sharma have proposed a solution for detection and prevention of wormhole attack in MANETs. They have introduced a trust based management scheme for computing a truthful path. They reveals that various solutions were proposed to avoid wormhole attack in mobile ad hoc networks. Further they categorized presently available approaches as; cluster based approaches, secure routing, trust based management approach, key management and intrusion detection system [15]. Researchers Mohit Soni, Manish Ahirwar and Shikha Agrawal were surveyed various intrusion detection techniques applied for MANETs. Their assessment states some intrusion detection systems available for conventional wired networks can be applied into mobile ad hoc networks also. Some of them include; standalone intrusion

detection system, distributed and cooperative intrusion detection system and hierarchical intrusion detection system [16].

Researchers Sunyanan Choochotkaew and Krerk Piromsopa were analysed different existing authentication models and proposed a global decision process which helps in deciding an authentication model for a particular MANET application [17]. Researchers Alka Chaudhary, V.N.Tiwari and Anil Kumar have proposed an "anomaly fuzzy fuzzy intrusion detection system" for detecting data packet sinking attacks in MANETs. This solution helps in removing malicious nodes from the network and in order to save resources associated with the mobile nodes [18]. Researchers Slavica V. Bostjancic Rakas and Valentina V. Timcenko were proposed MPBM (MANET Policy Based Management System). Proposed MPBM is an automated solution for overall policy based management in MANETs. The MPBM consists of four units namely; configuration, security, QoS (Quality of Service) and network resources [19].

Researchers Yaser M. Khamayseh, Shadi A. Aljawarneh, and Alaa Ebrahim Asaad and have studied "survivability against blackhole attacks in MANETs". They proposed a mechanism which build willing atmosphere to monitor and detect the behaviour of active transmission. In this solution, the source node uses rest nodes of the network as observer nodes to monitor the active transmissions. In case any error occurs, the observer node sends an error message to the source node. Upon receiving repetitive error messages from the observer node, the source node symbols the detected intermediate network node as a blackhole [20]. Researchers Paramjit Singh Waraich and Neera Batra were proposed a solution for DoS, blackhole, grayhole and sybil attacks for vehicular ad hoc networks, they proposed a quick response table to trace packet drops. Packet drops caused due to unknown reasons were taken into account to discard that particular route for any possible attack [22].

Researchers Mukesh Muwel, Prakash Mishra, Makarand Samvatsar and Upendra Singh were proposed an "Efficient ECGDH Algorithm through protected Multicast Routing Protocol in MANETs". They worked on multicast protocols to address man in the middle or sessional hijacking attacks [23]. Researchers Srinivas Aluvalaa, Dr. K. Raja Sekharb and Deepika Vodnalac were studied "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks. They analysed needs of detecting and preventing security attacks in time before they obstruct smooth functioning of the network [24]. Researchers T.H.Lacey, R.F.Mills, B.E.Mullins, R.A.Raines, M.E.Oxley and S.K.Rogers were proposed a reputation based multilayer security for MANETs. They examined the reputation based IPS (Internet Protocol Security) frame work for mobile ad hoc networks that functions in a hostile atmosphere. This research was inclined towards subsections of the global security challenges [25].

6. CONCLUSION

This paper reviews security challenges associated with the process of routing in mobile ad hoc networks. Here, we have studied different network layer attacks and primarily focused on routing attacks. Fundamental requirements of an ideal security aware routing protocol have been sketched. Various types of routing attacks have been surveyed with some well-known security solutions available so for. Previously and recently proposed solutions were studied separately in different sections. It is concluded that the security solutions proposed so for are limited to some well-known routing protocols in mobile ad hoc networks. There are numerous routing protocols available for mobile ad hoc networks. This paper will help researchers, scientists and engineers in providing better security solutions to other MANET routing protocols also.

REFERENCES

[1] C.S. Murthy and B.S. Manoj, "Ad Hoc Wireless Networks: Architecture and Protocols," Pearson Education Inc., Dorling Kindersley Publishing Inc., ISBN 81-317-0688-5.

[2] Shilpi Burman Sharma and Nidhi Chauhan, "Security issues and their solutions in MANET," IEEE 1st International Conference on Futuristic trend in Computational Analysis and Knowledge Management (ABLAZE-2015), 25-27 February, Noida, India, pp. 289-294. 2015. DOI: 10.1109/ABLAZE.2015.7155013.

[3] Priyanka Yadav and Muzzammil Hussain, " A Secure AODV Routing Protocol with Node Authentication," IEEE International Conference on Electronics, Communication and Aerospace Technology (ICECA 2017), 20-22 April, Coimbatore, India, pp. 489-493. 2017. DOI: 10.1109/ICECA.2017.8203733.

[4] B.Awerbuch, D.Holmer, C.Nita-Rotaru and H.Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the ACM Workshop on Wireless Security 2002, pp. 21-30. September 2002.

[5] Y. Hu, A. Perrig and D.B. Johnson, "Packet Leashes: A Defence Against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedingsof IEEE INFOCOM 2003, vol. 3, pp. 1976-1986. April 2003.

[6] Y. Hu, A. Perrig and D.B. Johnson, "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security 2003, pp. 30-40. September 2003.

[7] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks," Proceedings of ACM MOBIHOC 2001, pp. 299-302. October 2001.

[8] Y.Hu, D.B.Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of IEEE WMCSA 2002, pp.3-13. June 2002.

[9] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M.B. Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proceedings of IEEE ICNP 2002, pp. 78-87. November 2002.

[10] C.E. Perkins and E.M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100. February 1999.

[11] Lakshman Naik. L, R.U. Khan and R B. Mishra, "Analysis of Node Density and Pause Time Effects in MANET Routing Protocols using NS-3," International Journal of Computer Networks and Information Security (IJCNIS – Mecs Publication), vol. 8, no. 12, pp. 9-17, 2016. DOI: 10.5815/ijcnis.2016.12.02.

[12] H.Deng, W. Li and D.P. Agarwal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, October 2002.

[13] Sajal Sarkar and Raja Datta, "A game theoretic framework for stochastic multipath routing in self-organized MANETs,"Pervasive and Mobile Computing (Elsevier), vol. 39, pp. 117-134, 2017. DOI: 10.1016/j.pmcj.2016.09.008.

[14] Shahjahan Ali, Prof. Parma Nand and Prof. Shailesh Tiwari, "Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique," IEEE International Conference on Computing, Communication and Automation (ICCCA2017), 5-6 May, Greater Noida, India, pp. 520-523. 2017. DOI: 10.1109/CCAA.2017.8229856.

[15] Pawan Kumar Sharma and Vishnu Sharma, "SURVEY ON SECURITY ISSUES IN MANET: Wormhole Detection and Prevention," IEEE International Conference on Computing, Communication and Automation (ICCCA2016), 29-30 April, Noida, India, pp. 637-640. 2016. DOI: 10.1109/CCAA.2016.7813799.

[16] Mohit Soni, Manish Ahirwar and Shikha Agrawal, "A Survey on Intrusion Detection Techniques in MANET," IEEE International Conference on Computational Intelligence and Communication Networks (CICN2015), 12-14 December, Jabalpur, India, pp. 1027-1032. 2015. DOI: 10.1109/CICN.2015.204.

[17] Sunyanan Choochotkaew and Krerk Piromsopa, "An Analysis of Authentication Models for MANETs," IEEE International Conference on Information Science, Electronics and Electrical Engineering (ISEEE2014), 26-28 April, Sapporo, Japan, pp. 1956-1960. 2014. DOI: 10.1109/InfoSEEE.2014.6946265.

[18] Alka Chaudhary, V.N.Tiwari and Anil Kumar, "Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks," IEEE International Advance Computing Conference (IACC2014), 21-22 February, Gurgaon, India, pp. 256-261. 2014. DOI: 10.1109/IAdCC.2014.6779330.

[19] Slavica V. Bostjancic Rakas and Valentina V. Timcenko, "Quality of service and security issues in MANET environment," IEEE 22nd Telecommunications Forum Telfor (TELFOR2014), 25-27 November, Belgrade, Serbia, pp. 419-422. 2014. DOI: 10.1109/TELFOR.2014.7034437.

[20] Yaser M. Khamayseh, Shadi A. Aljawarneh and Alaa Ebrahim Asaad, "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency," Elsevier, Sustainable Computing: Information and Systems (SUSCOM-175), pp. 1-11. 2017. DOI: 10.1016/j.suscom.2017.07.001.

[21] YIH-CHUN HU and ADRIAN PERRIG, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Springer, Wireless Networks, vol. 11, pp. 21-38. 2005.

[22] Paramjit Singh Waraich and Neera Batra, "Prevention of Denial of Service Attack Over Vehicle Ad hoc Networks using Quick Response Table," 4th IEEE International Conference on Signal Processing, Computing and Control (ISPCC2017),21-23 Sepetember, Solan, India, pp. 586-591. 2017. DOI: 10.1109/ISPCC.2017.8269746.

[23] Mukesh Muwel, Prakash Mishra, Makarand Samvatsar and Upendra Singh, "Efficient

ECGDH Algorithm through protected Multicast Routing Protocol in MANETs," IEEE International Conference on Electronics, Communication and Aerospace Technology, (ICECA2017), 20-22 April, Coimbatore, India, pp. 631-637. 2017. DOI: 10.1109/ICECA.2017.8212743.

[24] Srinivas Aluvalaa, Dr. K. Raja Sekharb and Deepika Vodnalac, "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks," Elsevier, Procedia Computer Science, vol.92, pp. 554-561. 2016. DOI: 10.1016/j.procs.2016.07.382.

[25] T.H.Lacey, R.F.Mills, B.E.Mullins, R.A.Raines, M.E.Oxley and S.K.Rogers, "RIPsec – Using reputation-based multilayer security to protect MANETs," Elsevier, Computers & Security, vol. 31, pp.122-136. 2012. DOI: 10.1016/j.cose.2011.09.005.