Review on Latest Certainty Issues in Mobile Ad-Hoc Networks

M.Kamarunisha,S.Gowri,P.Anitha

**Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.*

Email: kamarunisha8891@gmail.com(**M.Kamarunisha**) *Corresponding author:* **M.Kamarunisha**

ABSTRACT

Mobile nodes communicate in a multi-hop mode in a MANET, which does not need access points or base stations. When it comes to security, the advantages of mobile ad-hoc networking far outweigh the disadvantages. This is because mobile nodes without adequate protection are vulnerable to compromise, static configurations may not be adequate for the dynamically changing topology in terms of security solutions, and lastly, lack of cooperation and limited capability are common in MANETs. An attacker with malicious intent may swiftly acquire access to the network due to the lack of clearly specified protective measures in MANET. The security of Mobile Ad-hoc Networks (MANETs) has been a popular issue in recent years, but there hasn't been much progress in developing the safest networks for these networks. This research paper provides an outline of the security issues and detection techniques for Mobile Ad Hoc Networks. The specific security issues posed by ad hoc networks will be discussed in this article, including the current security threats and the implementation of security services and attack countermeasures.

Mobile nodes communicate in a multi-hop mode in a MANET, which does not need access points or base stations. When it comes to security, the advantages of mobile ad-hoc networking far outweigh the disadvantages. This is because mobile nodes without adequate protection are vulnerable to compromise, static configurations may not be adequate for the dynamically changing topology in terms of security solutions, and lastly, lack of cooperation and limited capability are common in MANETs. An attacker with malicious intent may swiftly acquire access to the network due to the lack of clearly specified protective measures in MANET. The security of Mobile Ad-hoc Networks (MANETs) has been a popular issue in recent years, but there hasn't been much progress in developing the safest networks for these networks. This research paper provides an outline of the security issues and detection techniques for Mobile Ad Hoc Networks. The specific security issues posed by ad hoc networks will be discussed in this article, including the current security threats and the implementation of security services and attack countermeasures.

Keywords: MANET, Security Threats, Denial of Service (DoS), Passive & Active Attack, etc

1. INTRODUCTION

In other terms, Mobile Ad Hoc Network (MANET) is a collection of wireless mobile communication devices or nodes that connect with one another without the need for a permanent infrastructure or centralised management. The nodes in MANET are in charge of finding other nodes to interact with on their own. Due to the restricted transmission range of wireless network interfaces, it may be essential for one wireless mobile node to solicit the help of other hosts in forwarding a packet to its destination. In addition to serving as a host, each wireless mobile node also acts as a router, passing packets to other wireless mobile nodes in the network that may not be in close proximity. In an ad hoc network, each node may find many pathways to another node by participating in an ad hoc routing protocol [1]-5].

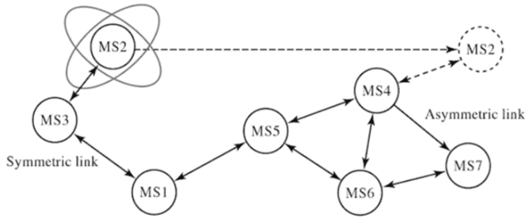


Fig 1: Mobile Ad Hoc Network (MANET)

2. COMMUNICATION IN MOBILE Network administration, packet forwarding, and routing are all handled by specialised nodes in conventional networks. It is possible that some received packets would become unusable due to network congestion, resulting in the need to retransmit even more packets. As a result, when networks are overloaded, the throughput of applications might drop to zero. This can lead to congestion collapse. In order to ensure high throughput and prevent congestion collapse, TCP employs a variety of methods. Slow start and congestion avoidance are two of the four linked algorithms that make up these systems.

- Contrasts the well-known one hop cellular network model, which depends on the cable backbone and stationary base stations to allow wireless communication between two mobile nodes [6]-[10].
- No such infrastructure exists in a MANET and the network topology may vary dynamically and unpredictably since nodes might relocate and each node has a limited transmitting power, which restricts access to the node only in the immediate vicinity.
- This diagram shows how information packets are carried in a "store and forward" fashion from one node to another, through intermediary nodes, in MANETs: a peer-to-peer, multihop wireless network.
- The connectedness of nodes may alter depending on the relative positions of other nodes as they move throughout the network. Network topology changes must be propagated across the network so that old information may be updated.
- It's important that other nodes in the network follow this new path for forwarding packets to MS2 when MS2's attachment point changes. All nodes in the illustration are assumed to be beyond the radio range of each other. Unless all nodes are within radio range of each other, there are no routing concerns.
- Asymmetric and symmetric (bidirectional and unidirectional) and asymmetric (bidirectional and unidirectional) linkages are raised in figures. If MS1 is within radio range of MS3, then MS3 is likewise within radio range of MS1. symmetric linkages with associative radio range Asymmetrical communication lines are in place. Due of variances in transmission power levels and geography, this assumption may not always be true Asymmetric network routing is a difficult problem to solve. In certain circumstances, asymmetric linkages may be avoided since it is difficult to locate the return path. In a MANET, efficiency is one of the many issues that need to be dealt with [11]-[15].
- The second problem is that various nodes have varied mobility patterns. There are also some nodes that are largely stable, while others are more or less movable.

2. MANET

- Ad hoc networks have the following characteristics:
- Nodes are allowed to move about in a dynamic topology, which means the network's structure may change at random and without warning. Bidirectional linkages are the primary component of dynamic topologies. A unidirectional connection may occur in certain instances when the transmission power of two nodes is different [16]-[20].
- With a limited bandwidth capacity, wireless networks continue to outperform their infrastructure counterparts.

- Depending on the MANET, some or all of the MSs may have to depend on batteries or other exhaustible sources of energy to power themselves. Energy saving may be the most significant design consideration for these nodes or devices.
- Wire-line networks, on the other hand, are less vulnerable to physical attacks than MANETs. An increase in the likelihood of eavesdropping and DoS attacks should be taken into account carefully. In wireless networks, a variety of connection security approaches are often used to decrease security risks.

2.2 Applications of MANET

- Cooperative mobile data sharing is an example of a specialised use of ad hoc networks in the industrial and commercial sectors. Despite the fact that military networks are constantly evolving, many of these networks demand strong, IP-compliant data services inside mobile wireless communication networks. For example, high data speeds, global roaming capabilities, and cooperation with other network topologies are allowing new applications in Mobile Ad Hoc Networks (MANs).
- Opportunities for education over the internet or in rural places due of the prohibitive cost of providing wire-line internet connectivity to all users in these areas.
- An increasing number of people are using ad hoc networks to provide emergency services and other information through a vehicle area network. This works equally well in urban and rural environments. The fundamental and essential information that is useful in a specific scenario is exchanged and discussed.

3. THREATS IN AUTOCONFIGURATION

The nodes that make up the MANET are intended to behave reliably and predictably in the procedures used during the implementation of the mechanisms of auto-configuration. However, malicious nodes may be inflicting some harm, such as interfering with communications, spoofing, denial of service, and eavesdropping, among other things. This is not always the case. Security hazards are defined in this study using a categorization system developed by Wang and Buiati et al.

First, there is a risk of address spoofing. It is possible for a rogue node to purposefully target a free or allocated IP address. When a malicious node pretends to be its victim, it hijacks the traffic of any other node that has been configured. When the node provides a free IP address to itself, it gathers information needed to carry out active assaults, such as denial of service.

(ii) Exhaustion of Addressable Space. Until the address space is exhausted, a rogue node may claim as many IP addresses as feasible. A ghost node's address may be requested via this node (fake nodes). In this method, the rogue node might block additional nodes from being setup and joining the MANET..

(iii) Deal with the Risk of Conflict. It is possible for a malicious node to provide a requester with a duplicate address from a list of addresses that are already in use. As a result, an AREP black hole attack will occur in the DAD process, resulting in an address conflict in the MANET.

(iv) Conflict Threat from a False Address. To avoid a conflict with the requester, a malicious node may respond to a request for an address in an unethical manner, utilising messages AREQ (address request) and fake addresses in messages AREP (address reply). Nodes would have to give up their current addresses if they couldn't verify the legitimacy of the new one. Attackers may modify their IP addresses to carry out their attacks.

In the event of a DDoS attack, In an auto setup procedure, a malicious node might pose as a requester and transmit AREQ messages to many initiator nodes concurrently. In the same way, a malicious node may transmit a large number of bogus DAD messages, resulting in an overburdening of the network with unnecessary data.

Threat (vi) of Sybil (Multiple Identity). Illegally claiming numerous identities, a node is doing so (Sybil node). Node may create a new identity, or it can hijack an existing valid node. It is possible for a Sybil node to request or acquire a large number of IP addresses.

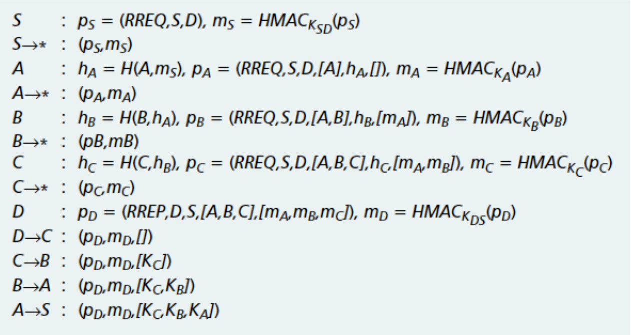
(viii) Threat of a Negative Response. When a new IP address is assigned, all preconfigured nodes must approve of it, and an attacker may submit a negative answer to prevent the new node from entering the network.

4. A MULTIFENCESECURITYSOLUTION

4.1 NETWORK-LAYER SECURITY

Designs for MANET-based networks' network-layer security Security proposals for MANETs are discussed in this section. Fig. 1 shows that the ultimate multi-hop security solution naturally covers both the network and link levels because of the distributed protocols used to offer multi-hop connection in MANETs. A MANET may be secured in two ways: proactive and reactive. The proactive method aims to prevent security risks by using a variety of cryptographic approaches. However, the reactive strategy aims to identify risks and respond to them after the fact. Each method has its own advantages and may be used to handle a wide range of problems in the field. While most secure routing systems employ the proactive technique to secure routing data between mobile nodes, the reactive approach is commonly used to safeguard packet forwarding operations. Security solutions for MANETs must include both proactive and reactive techniques, and include all three components: prevention, detection, and response, since there is no obvious line of defence. The attacker is deterred by a large increase in the difficulty of breaching the system as a result of the preventive component. No matter how meticulously the preventive methods are developed, experience has demonstrated that no system can be absolutely free of incursion. A mobile-device-based network (MANET) is particularly vulnerable to compromise or physical capture because of the devices that make up MANETs. In order for security systems to function in the context of limited intrusions, the detection and response components that uncover occasional incursions and take measures to prevent lasting detrimental consequences are essential. Secure ad hoc routing protocols in the MANET environment are primarily responsible for preventing the attacker from installing wrong routing states on other nodes. DSR [2] and AODV[1] are two examples of previous ad hoc routing protocols that utilise various
safeguard the network's ability to transport packets across mobile nodes via multi-hop ad-hoc forwarding. It's important that each router's packet forwarding behaviour and the routing message it sends be in sync with one another, therefore they're working hard to achieve this goal. Secure packet forwarding protocols and secure ad hoc routing protocols Authentication Code (message authentication codes). 1 A cryptographic one-way hash function h can quickly and efficiently construct and validate a message authenticator hK() when two nodes share a secret symmetric key K. Even low-end devices, such as sensor nodes, may benefit from the efficient computing. A broadcast message cannot be authenticated using an HMAC since it can only be validated by the intended recipient. Furthermore, creating a secret key between two nodes is a difficult task. In a network of nodes, a total number of keys will be preserved if the pairwise shared key is employed. Using pairwise shared keys, SRP for DSR implements this strategy.

.



$$
\begin{array}{lcl}
S & : & p_S = (RREQ,S,D),\ m_S = HMAC_{K_{SD}}(p_S) \\
S \rightarrow * & : & (p_S,m_S) \\
A & : & h_A = H(A,m_S),\ p_A = (RREQ,S,D,[A],h_A,[]),\ m_A = HMAC_{K_A}(p_A) \\
A \rightarrow * & : & (p_A,m_A) \\
B & : & h_B = H(B,h_A),\ p_B = (RREQ,S,D,[A,B],h_B,[m_A]),\ m_B = HMAC_{K_B}(p_B) \\
B \rightarrow * & : & (pB,mB) \\
C & : & h_C = H(C,h_B),\ p_C = (RREQ,S,D,[A,B,C],h_C,[m_A,m_B]),\ m_C = HMAC_{K_C}(p_C) \\
C \rightarrow * & : & (p_C,m_C) \\
D & : & p_D = (RREP,D,S,[A,B,C],[m_A,m_B,m_C]),\ m_D = HMAC_{K_{DS}}(p_D) \\
D \rightarrow C & : & (p_D,m_D,[]) \\
C \rightarrow B & : & (p_D,m_D,[K_C]) \\
B \rightarrow A & : & (p_D,m_D,[K_C,K_B]) \\
A \rightarrow S & : & (p_D,m_D,[K_C,K_B,K_A])
\end{array}
$$

In a network of n nodes, it is necessary to maintain. It is the digital signature technique used by SAODV [6] and ARAN [7]. This is a one-way HMAC keyring. It is computationally infeasible to identify the input x for many crypto-graphic one-way functions. It is possible to build up a chain of output fis by repeatedly performing f(x) on x. (x). In the opposite sequence of creation, these outputs may be used to authenticate messages: a message with an HMAC utilising fi(x) as the key is confirmed legitimate when the sender exposes fi–1 (x). TESLA [14] is an example of a hash-chain-based broadcast message authentication mechanism. Ariadne (DSDV), SEAD (DSDV), and packet leashes (wormhole) all use this strategy. One authenticator can be validated by a large number of receivers using one-way key-chain-based authentication. However, there is a price to pay for these advantages. As a first step, hash-chain-based authentication needs hardware capabilities for precise clock synchronisation. A message is needed for verification by the recipients when the key is exposed. Routing protocol responsiveness may be severely impacted by a delay in verifying routing messages. A huge amount of storage and very precise clock synchronisation are required for instant authentication (e.g., TIK [8]). To finish things off, a second round of conversation is necessary before the key may be released. Timer calibration is critical for each situation. The storing of the hash chain is difficult for lengthy chains, which are necessary in scenarios with longer keying intervals.

4.2 SECUREADHOCROUTING

For DSR, Ariadne [5] is a safe extension. For message authentication, it makes use of a one-way HMAC key chain (i.e. TESLA). The sender's TESLA key chain is presumed to include the latest released key by the receiver, as a result of key management and distribution. As an example, consider the following scenario: Using three intermediary nodes (A, B, and C), the source node S connects to the destination node D. By using a key shared by Sand D and C, HMACKSD(M) represents message M's HMAC code created by the protocol, a hash chain is established at the destination. Hash functions H and HMACKSD(S, D) verify the chain's contents and the source-destination relationship, respectively. According to Fig. 2, where * signifies a local broadcast, HMACX() denotes the HMAC code produced on node X, the propagation of the route request (RREQ) and response (RREP) messages can be shown. D can calculate mS at the destination since pS information is present in pC. According to pC's explicit node list, D dynamically computes the hC value and compares this hC to the embedded hC for forgery detection. You don't require an authentication code for each and every RREP packet during the RREP phase. Any forwarder X who has previously committed the one-way function outputs mX= HMACKX() at the RREQ phase; then at the RREP phase, mXKX is fulfilled by providing the key to the one-way function, which is the trapdoor commitment.

4.3 DISTANCE VECTOR ROUTING

Each intermediate node must appropriately publicise the routing metrics for distance vector routing protocols like DSDV and AODV in order for them to work. This means that each node must raise its hop count by precisely one if the routing metric is using this method. An intermediary node can't lower the hop count in a routing update because of a hop count hash chain [6, 15] that's been designed. Unlike one-way HMAC key chains for authentication, a hash chain for this purpose does not need temporal synchronisation. Figure 2 shows that every time a node launches an RREP message, it produces a hash chain of length n. Messages exchanged between Ariadne and its secure routing system in this order.

5. RELATED WORKS IN SECURITY SYSTEM FOR MANET

A mechanism for multiple route reply forwarding and filtering was developed by Noguchi and Hayakawa in 2018. A black hole attack on the network is addressed using this strategy. This approach uses the AODV routing protocol to determine the network's packet delivery ratio (PDR), throughput, and overhead. Using this strategy, the source node will request the highest sequence number of the RREP packet for a certain RREQ packet after checking the threshold value of the attacker node. The average quality of the route between the source and the destination node will also be checked. It is possible to fix PDR, throughput and overhead concerns of the network at considerably greater rates with the use of these solutions.

TBS, SDR, and MAODV routing protocols were employed by Swain, Pattanayak, and Pati in 2017. With these routing methods, rogue nodes may be eliminated while simultaneously increasing PDR and reducing network power consumption. According to the author, the TBS routing protocol is superior to both SDR and MAODV. It uses less power with lower delay rates and provides a greater PDR factor with the TBS protocol.

AODV and DSR routing protocols were developed on by Reda, Azer, in 2017. As a result of these protocols, packet loss rates and the proportion of network nodes capable of defending themselves against attacker nodes were determined. Two scenarios have been created for this purpose, one in regular mode and the other with malevolent attackers. In normal mode, AODV performs better since it maintains its cache. Both AODV and DSR will discard packets when a malicious node is found, however AODV has a better result because of its reactive nature.

Tactical MANET, or T-MANET, was studied by Shabut, Dahal, Kaiser, and Hossain in 2017. For detecting reasons, it is employed in cars, autos, and stations. T-most MANET's critical difficulties, such as the harm caused by black holes, grey holes, and selfish nodes, are addressed using the DSR routing protocol. The DSR protocol is employed because it may increase the network's PDR and throughput parameters. Detection method, cryptography detection, and trustworthy detection are some of the strategies employed by the author[22-31]. With these approaches, black hole and grey hole exhibit comparable results but selfish node delivers superior results, i.e., greater PDR and throughput on all techniques, and vice versa.

H-MANET, or heterogeneous and homogeneous MANET, was developed by Rishiwal, Agarwal, and Yadav in 2016. Researchers employed AODV routing to uncover scalability, lower energy scenarios, and heterogeneity in their study. While just the delay in a homogeneous MANET can be kept after the simulation is complete, the results of a heterogeneous network show greater PDR and throughput, as well as a bigger number of active nodes and a lower energy usage.

It has been shown that Matre and Karandikar, 2016 have done research on the modified on-demand on-demand multicast distance vector routing protocol (MAOMDV) and the AODV. MANET's security benefits from this. MAOMDV routing protocol made use of cryptographic patterns to keep data safe. Negative occurrences, good events, and public opinion were all taken into consideration while determining the three metrics employed. Routes promote communication between nearby nodes in positive events. Negative occurrences cause the route to dislocate, and no information is available about the next node on the path. Whereas network security guarantees that data is sent or delivered securely. MAOMDV's PDR and throughput increase as the number of nodes and area grows, while the delay factor decreases. I make a comparison to AODV.

Game theory using dynamic bayesiansignalling game (DBSG) and perfect bayesian equilibrium theory (PBE) together with AODV, CBRP, and SRP-GM routing protocol were employed by Paramasivan, Prakash, and Kaliappan., 2015. With this technology, hostile nodes may be located and eliminated from the network as well as node utility, strategy, and performance bottlenecks. DBSG is more successful at locating malicious nodes and transmitting and receiving data in a certain time frame, while PBE conducts the same procedure but with a bigger delay. This technique models this difference.

Sari, in 2014, worked on USM and RAS, i.e. utility sensor mechanism and rate adaptation method using AODV routing protocols. IEEE 802.11 and DCF sections of the data connection layer may benefit from these techniques to enhance throughput and latency. DDOS and jamming assaults in the network will be reduced as a result of this. For modifications and detecting mechanisms, these two strategies are highly recommended to a significant degree, which can manage the PDR, throughput and delay factor all at the same time Available online at https://ssrn.com/abstract=3356214 (in PDF format). 26-28 February 2019, SUSCOM-2019, International Conference on Sustainable Computing in Science, Technology and Management | In India, Jaipur is home to Amity University Rajasthan. On the 1468th page

Authenticated routing ad hoc network with zone routing protocol (ARAN-Z) has been developed by Khalil, Bataineh, Qubajah, and Khreishah in 2013. This novel routing protocol is compared to the basic ARAN and ZRP routing protocols. A network's optimal PDR, routing load (measured in bytes and packets), average route length, and latency may be determined in this way, among other things. The more mobile and dense a network is, the more likely an attacker node is to do damage. ARAN-Z, on the other hand, achieves superior outcomes because to its greater PDR and lower latency when the routing load factor increases as compared to ARAN and ZRP.

As part of their work in 2013, Ganesh and Amutha developed a new routing system, one that is both efficient and secure (ESRPSDC). This is done to ensure that the wireless sensor network's energy consumption is kept to a minimum. In a wireless sensor network, there is no guarantee of node security or reliability. It's possible for a malicious node to attack the network at any moment and do damage. PDR, delay with network load, and the number of malicious nodes in the network are all analysed in this study using this innovative routing protocol. PDR is increased and latency is reduced with a lower SNR ratio as a result of the ESRPSDC routing protocol.

Conclusions and Recommendations

This article has attempted to explain what MANETs are, what they can do, and how they can be used. Different criteria for evaluating the network's safety are also implemented. There is a lot of attention paid to MANETs' weaknesses and probable attacks. The study of the above provides a thorough grasp of the potential issues that may arise in MANETs. It aids in the selection of an appropriate method for solving the situation at hand. Security measures will be examined in depth in a final report that outlines all of the viable options. A closer look at the approaches and flaws of current systems will help researchers get a clearer picture of how to continue in the development of a better system with more advanced capabilities.

6. REFERENCES

[1] C. Perkins and E Royer, “Ad Hoc On-Demand DistanceVector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[2] D. Johnson and D. Maltz, “Dynamic Source Routing inAd Hoc Wireless Networks,” Mobile Computing, T.Imielinski and H. Korth, Ed., Kluwer, 1996.

[3] EEE Std. 802.11, “Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications,” 1997.

[4] B. Schneier, Secret and Lies, Digital Security in a Net-worked World, Wiley, 2000.

[5] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A SecureOn-demand Routing Protocol for Ad Hoc Networks,“ACM MOBICOM, 2002.[6] M. Zapata, and N. Asokan, “Securing Ad Hoc RoutingProtocols,” ACM WiSe, 2002.

[6] Mobile Adhoc Network (MANET). Routing Protocol Performance Issues and Evaluation Considerations. URL: http://www.ietf.org/rfc/rfc2501.txt

[7] S. Basagni et al., Mobile Ad Hoc Networking, IEEE Press and John Wiley and Sons, 2003.

[8] Conti, M.; Maselli, G.; Turi, G.; Giordano, S.; , “Cross-layering in mobile ad hoc network design,” Computer , vol.37, no.2, pp. 48- 51, Feb 2004, doi: 10.1109/MC.2004.1266295 URL: http://ieeexplore.ieee.org/ stamp/stamp.jsp?tp= andarnumber = 1266295andisnumber=28321
CrossRef

[9] Chakrabarti, S.; Mishra, A.;, “QoS issues in ad hoc wireless networks,” IEEE Communications Magazine, vol. 39, no.2, pp.142-148, Feb 2001, doi: 10.1109/35.900643 URL: http://ieeexplore.ieee.org/

stamp/stamp.jsp?tp=andarnumbe r=900643andisnumber =19494
CrossRef

[10] Royer, E.M.; Chai-Keong Toh; , “A review of current routing protocols for ad hoc mobile wireless networks,” IEEE Personal Communications, vol.6, no.2, pp.46-55, Apr 1999, doi: 10.1109/98.760423 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber= 760423andisnumber=16455\
CrossRef

[11] J. Macker, ”Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”. IETF RFC 2501, January 1999.

[12] Mohammed Saeed Al-kahtani, “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs),” IEEE 2012.

[13] Gagandeep, Aashima, Pawan Kumar,“ Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[14] Priyanka Goyal, Sahil Batra, Ajit Singh “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010

[15] Amitabh Mishra and Ketan M. Nadkarni, “Security in Wireless Ad Hoc Networks”, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[16]Lidong Zhou and Zygmunt J. Hass, “Securing Ad Hoc Networks”, IEEE Networks Special Issue on Network Security, November /December 1999. Google Scholar

[17]Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005. Google Scholar

[18] Yau P.-W., Mitchell C.J., “Security Vulnerabilities in Ad Hoc Networks”, In Proc. of the 7th Int. Symp. on Communications Theory and Applications, pp. 99-104, 2003. Google Scholar

[19] Jim Parker, Anand Patwardhan, and Anupam Joshi, “Detecting Wireless Misbehavior through Cross-layer Analysis,” in Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC’2006), Las Vegas, Nevada, 2006. Google Scholar

[20] Panagiotis Papadimitraos and Zygmunt J. Hass, “Securing Mobile Ad Hoc Networks”, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003. Google Scholar

[21] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, in Proceedings of ICNP’02, 2002.

[22] Remya, R. R., Samrot, A. V., Kumar, S. S., Mohanavel, V., Karthick, A., Chinnaiyan, V. K., ... & Muhibbullah, M. (2022). Bioactive Potential of Brown Algae. Adsorption Science & Technology, 2022.

[23] Remya, R. R., Julius, A., Suman, T. Y., Mohanavel, V., Karthick, A., Pazhanimuthu, C., ... & Muhibbullah, M. (2022). Role of Nanoparticles in Biodegradation and Their Importance in Environmental and Biomedical Applications. Journal of Nanomaterials, 2022.

[24] Madavan, R., Saroja, S., Karthick, A., Murugesan, S., Mohanavel, V., Velmurugan, P., ... & Sivakumar, S. (2022). Performance analysis of mixed vegetable oil as an alternative for transformer insulation oil. Biomass Conversion and Biorefinery, 1-6.

[25] Mohanavel, V., Ravichandran, M., Anandakrishnan, V., Pramanik, A., Meignanamoorthy, M., Karthick, A., & Muhibbullah, M. (2021). Mechanical properties of titanium diboride particles reinforced aluminum alloy matrix composites: a comprehensive review. Advances in Materials Science and Engineering, 2021.

[26] Raja, T., Ravi, S., Karthick, A., Afzal, A., Saleh, B., Arunkumar, M., ... & Prasath, S. (2021). Comparative Study of Mechanical Properties and Thermal Stability on Banyan/Ramie Fiber-Reinforced Hybrid Polymer Composite. Advances in Materials Science and Engineering, 2021.

[27] Gurusamy, P., Sathish, T., Mohanavel, V., Karthick, A., Ravichandran, M., Nasif, O., ... & Prasath, S. (2021). Finite element analysis of temperature distribution and stress behavior of squeeze pressure composites. Advances in Materials Science and Engineering, 2021.

[28] Dharmaraj, R., Karthick, A., Arunvivek, G. K., Gopikumar, S., Mohanavel, V., Ravichandran, M., & Bharani, M. (2021). Novel approach to handling microfiber-rich dye effluent for sustainable water conservation. Advances in Civil Engineering, 2021.

[29] Aravindh, M., Sathish, S., Prabhu, L., Raj, R. R., Bharani, M., Patil, P. P., ... & Luque, R. (2022). Effect of various factors on plant fibre-reinforced composites with nanofillers and its industrial applications: a critical review. Journal of Nanomaterials, 2022.

[30] Uthirasamy, R., Chinnaiyan, V. K., Vishnukumar, S., Karthick, A., Mohanavel, V., Subramaniam, U., & Muhibbullah, M. (2022). Design of boosted multilevel DC-DC converter for solar photovoltaic system. International Journal of Photoenergy, 2022.

[31] Chandrika, V. S., Thalib, M. M., Karthick, A., Sathyamurthy, R., Manokar, A. M., Subramaniam, U., & Stalin, B. (2021). Performance assessment of free standing and building integrated grid connected photovoltaic system for southern part of India. Building Services Engineering Research and Technology, 42(2), 237-248.