iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XII **Month of publication:** December 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Routing Protocols and Vulnerabilities in Mobile Ad-Hoc Network (MANETs)

Shilpa Gambhir[1], Karishma Bajaj[2], Shashank Singh[3]
[1,2,3]*Assistant Professor, ECE Department*
MM University, Sadopur, Ambala, Haryana

Abstract— Mobile ad hoc network (MANET) is composed of a collection of mobile nodes which are movable. Therefore, dynamic topology, unstable links, limited energy capacity and absence of fixed infrastructure are special features for MANET when compared to wired networks. MANET does not have centralized controllers, which makes it different from traditional wireless networks (cellular networks and wireless LAN). An adhoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it then address the possible solution to protect the security mechanism, which involve Availability, integrity, authentication and non-repudiation. Finally a comparison of various routing protocols in MANETs is presented.
Index Terms- MANET, Power utilization, routing, attacks, threats.

I. INTRODUCTION

MANETs are formed by mobile nodes communicating with each other through wireless links without any governing body [1]. These mobile nodes can be Personal Digital Assistants (PDAs), laptops, cell phones that communicate with each other without any fixed infrastructure and central management as shown in figure 1. In circumstances where mobile telephony as we know it is not possible or difficult, perhaps internet technology can be of help.

Figure 1. Mobile Adhoc Network (MANET)

A mobile ad hoc network (MANET) is a wireless mobile node that frequently organizes in personal and temporary network in different way. In the mobile ad hoc network, nodes can easily communicate with all the other nodes within their frequency ranges [2]. Mobile Ad-hoc Network (MANET) is a collection of in- dependent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of

any infrastructure. This property makes these networks highly flexible and robust.

A. Characteristics of MANETs

Communication via wireless means.
Nodes can perform the roles of both host and router
No centralized controller and infrastructure.
Intrinsic mutual trust.
Dynamic network topology.
Frequent routing updates.

B. Advantages and Applications

The following are the advantages of MANETs:

They provide access to information and services regardless of geographic position.

These networks can be set up at any place and time.

The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. It includes:

Military or Police Services

Sensor Networks

Medical Service

Personal Area Network.

Disaster relief operations

Urgent Business meetings

Mine cite operations

II. PROBLEM FORMULATION

Vulnerability or Threat is a weakness to security of the network or system which allows an attacker to harm the confidential information. A MANET is a self-organizing network, packet forwarding etc. are performed by the nodes of the network themselves. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered.[3]. So security of the network is major challenge. Following are the challenges faced in MANETs:

A. Restricted Power Supply in MANETs

One important aspect of ad-hoc networks is power efficiency since only a simple battery provides nodes independence. Thus, minimizing power consumption is a major challenge in these networks. Power consumption is one of the most important performance metrics for wireless ad hoc networks, it directly relates to the operational lifetime of the networks.[4] Mobile elements have to rely on finite source of power while battery technology is improving over time, the need for power consumption will not reduce. This point will have a harmful effect on the operation time as it will have on the connection quality and bandwidth. In MANETs, every node has to perform the functions of a router. So if some nodes die early due to lack of power so that the network

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

becomes disjointed, then it may not be possible for other nodes in the network to communicate with each other. In the Wireless Ad-hoc Networks, battery replacement may not be possible. So as far as power consumption concerned, we should try to save power while maintaining high connectivity.

B. Lack of Adjacent Nodes in MANETs

MANETs have the ability to change of wireless connections between nodes. Because the limited energy provide for the wireless nodes and the mobility of the nodes, the wireless connection between mobile nodes in the ad hoc network are not regular for the communication participants[4]. The nodes can regularly move into and out of the frequency range of the other nodes in the ad hoc network, and the routing information will be converting all the time because of the action of the nodes.

C. Scalability

Due to mobility of nodes, scale of adhoc network changing all the time [5], [6]. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

D. Lack Of Centralized Management Facility

Mobile ad hoc network doesn't have a centralized monitor server. Firstly the absence of management makes the detection of attacks hardly because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network [7]. Lack of centralized management will block trust management for nodes. Second, shortage of centralized management machinery will block the secure management for the nodes in the ad hoc network.

E. Attacks In MANETs

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it.

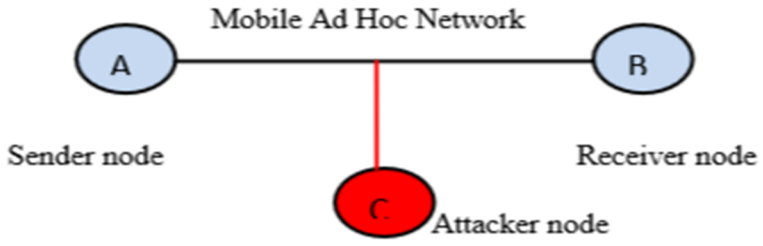


Figure 2: A passive attack where the attacker hears the messages on the links in usage.

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. They can physically damage a node to terminate its operation from the network, can capture the messages to modify and replay the messages back in the network; they can also disrupt the normal routing scheme, and can consume the network resources such as bandwidth, memory, computational power, and energy.

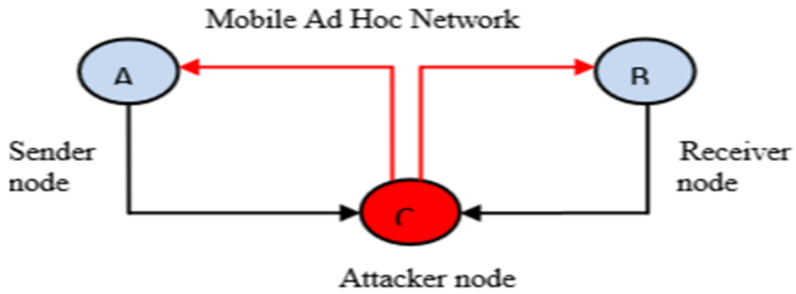


Figure 3: An active attack where the attacker alters the network operation.

Active attacks can be internal or external.

1) External Attacks: The attacker's main objective is to cause congestion, broadcast false routing information or disrupt nodes from providing services [8].

2) Internal Attacks: The malicious entity wants to obtain the normal access to the network and take part in the services of network either by some malicious intuition to get the access to the network as a new node, or by directly compromising a current node and using it as a base to perform its malicious actions.

F. Stingy Resources

As the resources available to the mobile nodes in a mobile ad hoc environment are not sufficient, the users become stingy while communicating. Due to limited bandwidth, higher cost, slower links and power constraints, the users, i.e., the mobile nodes may be lured for these constraints by the attackers and therefore such stingy resources may make the network vulnerable to attacks[7].

G. Bandwidth Constraint

The wireless networks have limited capacity links, and therefore, they are more vulnerable to environmental disturbances, which can degrade the quality of service of the network. They are more prone to external interferences, external noise, signal attenuation etc.

III. ROUTING PROTOCOLS

Classification of MANET routing protocols is done in following ways:

A. Unicast Routing Protocols

The routing protocols that consider sending information packets with a single destination from the single source [8].

B. Multicast Routing Protocols

Multicast may be the delivery of knowledge to your list of destinations simultaneously, while using well organized technique to deliver the messages over each link with the network just once, creating copies as long as the links for the destinations split [8].

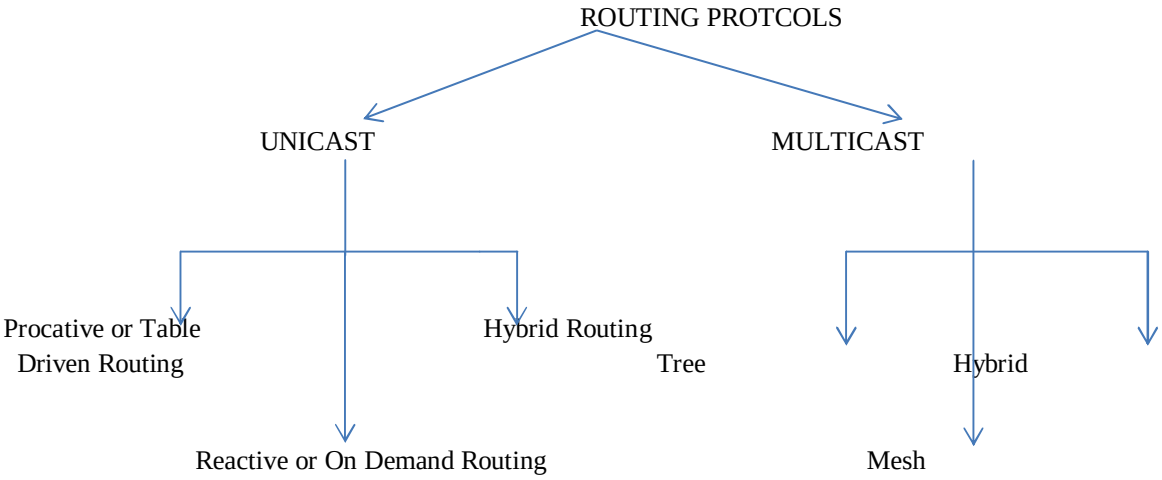


Figure 4: Classification of Routing Prtocols

There are basically three kinds of Unicast routing protocols which are:

Proactive routing protocols continuously learn the changes in the topology within a network by exchanging real-time topological information among the neighboring network nodes. Therefore, whenever there is a requirement arises for a route from source to destination node, such routing information is available immediately to the source node. Frequently changing network topology

could increase the overall cost of maintaining the network. But, if the network topology changes are slow, the information about change in topology might even not be used, reducing the overall cost of maintaining the network. Proactive routing protocols may also be called as table driven routing protocols. With this every node maintain routing table which contains details about the topology even without requiring it [5]. This useful feature for datagram traffic, brings significant signalling traffic and consumption of power [6]. The routing tables are updated periodically whenever the topology changes. Some of the table driven routing protocols are as follows:

Dynamic Destination-Sequenced Distance-Vector Routing Protocol: DSDV [8] is developed by Bellman-Ford routing [9] algorithm by modifications. Therein routing protocol, each mobile node within the network keeps a routing table. Each one of the routing table provides the directory all available destinations and the number of hops to every. Each table entry is tagged which has a sequence number, which can be originated because of the destination node.

Global State Routing (GSR) protocol [10], nodes during routing information exchange, shares their vectors of link states among their neighbouring nodes. Nodes maintain their global information depending on their link state vectors; this gives them information about their topologies so that they can locally optimize their routing decisions

Wireless Routing Protocol : WRP [9] is among the general class of path-finding algorithms [8, 10, 11], looked as the number of distributed shortest path algorithms that calculate the paths using information regarding the length and second-to-last hop with the shortest road to each node.

Some other proactive routing protocols are Cluster Gateway Switch Routing Protocol (CGSR), Hierarchical State Routing (HSR), Fisheye State Routing (FSR) and Zone-Based Hierarchical Link State (ZHLS)

Reactive or On Demand Routing Protocols: These protocols are known to have a little lazy approach. They do not update their routing tables periodically unless it is demanded by any node. They aren't suitable for the networks that are highly dynamic and prone to frequent changes. The lives of the route entries in routing tables of the nodes are until the routes are no longer needed. The routes are decided on the basis of the shortest path [12]. While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used.

AODV: AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best features of AODV is to provide broadcast, unicast, and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

DSR: The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power. In order to identify link layer failure DSR needs support from the MAC layer. It is consist of the two network processes, Route Discovery and Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

TORA: Temporarily Ordered Routing Algorithm is an adaptive, scalable and efficient distributed routing algorithm. It is mainly designed for multi-hop wireless networks as well as highly dynamic mobile environment. It is also called source-initiated on-demand routing protocol. It is also use to find multiple routes from source to destination node. One of the main features is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. It has three basic functions: Route maintenance, Route erasure and Route creation [13].

Some other reactive routing protocols are Associativity-Based Routing (ABR), Signal Stability-Based Adaptive Routing Protocol (SSA), Cluster-Based Routing Protocol (CBRP)

Hybrid routing protocols: It exploits the characteristics of both the reactive and proactive routing protocols to get the better results.

It combines the two different protocols in a way unique way. It arranges the network into zones, it uses proactive protocol with in a zone and reactive to route the packets in the nodes of different zones.In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on- demand routing protocols [11], [14].

Zone Routing Protocol (ZRP): Zone Routing Protocol [14] is acceptable for wide selection of MANETs, for the networks with large coverage and diverse mobility patterns. Within this protocol, each node pro-actively maintains routes with a local region, and that is known as routing zone. Route creation is performed by using a query-reply mechanism.

Dual-Hybrid Adaptive Routing (DHAR): DHAR [13] uses the Distributed Dynamic Cluster Algorithm (DDCA) presented in [31]. The concept of DDCA is to partition the network in real-time, into some non-overlapping clusters of nodes. In DHAR, routing is completed using a dynamic two-level hierarchical process, including optimal and less-complicated table-driven algorithms operating at every level.

Neighbor-Aware Multicast Routing Protocol :NAMP [12] can be a tree-based hybrid routing protocol, which utilizes neighbor-hood information. The routes within the network are planned and maintained via traditional request and reply messages or based-on demand. This hybrid protocol uses neighbor information of two-hops away for transmitting the packets towards the receiver.

Some other Hybrid routing protocols are Sharp Hybrid Adaptive Routing Protocol (SHARP) and Adaptive Distance Vector Routing (ADV)

Multicast Routing Protocols are of following types:

Tree-based multicast routing protocol establishes and maintains a shared multicast routing tree to deliver data from a source to receivers of a multicast group. A well-known example of treebased multicast routing protocols are the Multicast Ad hoc on demand Distance Vector routing protocol (MAODV).

Mesh-based multicast routing protocol sustains a mesh consisting of a connected component of the network containing all the receivers of a group. Example of mesh-based multicast routing approaches is On-Demand Multicast Routing Protocol (ODMRP).

Hybrid Multicast routing is the type of protocols which have the combination of both tree-based and mesh-based multicasting routing protocols.

IV. SECURITY SOLUTIONS TO THE MOBILE AD HOC NETWORKS

Security Criteria: We have discussed several routing techniques that potentially make the mobile ad hoc networks in secure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

A. Availability

It ensures that the intended network security services listed above are available to the intended parties when required. The availability is typically ensured by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocols [8].

B. Integrity

It ensures that the data has not been altered during transmission. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

C. Confidentiality

It ensures that the intended receivers can only access transmitted data. This is generally provided by encryption.

D. Authenticity

Both sender and receiver of data need to be sure of each other's identity. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates. Details of the construction and operation of digital signatures

can be found in RFC2560.

E. Non-Repudiation

Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. Non-repudiation requires the use of public key cryptography to provide digital signatures. A trusted third party is required to provide a digital signature [10].

F. Authorization

is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions [15].

G. Anonymity

means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software.

Table 1 presents comparison of various routing protocols

PARAMETER	PROACTIVE OR TABLE DRIVEN PROTOCOLS	REACTIVE OR ON DEMAND PROTOCOLS	HYBRID ROUTING PROTOCOLS
INFORMATION OF ROUTING	Already stored in routing table	Not stored anywhere	May or may not be stored depending upon zone.
AVAILABILITY OF ROUTES	Always available	May or may not be available depending upon requirement	Depends on location of zone
MEMORY REQUIREMENT	More as table is maintained	Less as routing information is not stored anywhere	Depends on routing information inside or outside zone
TRAFFIC CONTROL	high	Low	lowest
SECURITY AGAINST	DoS attacks	Resource depletion attacks, spoofing attacks and jamming attacks	Eavesdropping and colluded attacks
SECURING METHOD OR FUNCTION	Uses Clock Synchronization method and TTP methods	Reputation mechanism for monitoring of the cooperativeness of nodes and mobile gateaways	Threshold Secret Sharing
NO. OF NODES	Upto 100 nodes	Above 100 nodes	More than 1000 nodes
DELAY	Low as no waiting for routes is done	Higher than procative	Depends, higher when inter zone and lower when confined zone
NETWORK ORGANIZATION	Hierarchical or flat	Flat	Both
TOPOLOGY DISTRIBUTION	Periodical	On demand	Both
TYPES	DSDV, WSR, GSR CGSR, HSR, FSR, ZHLS	TORA, AODV, DSR, ABR, SSA, CBRP	ZRP,DHAR, NAMP, SHARP, ADV

TABLE 1: Comparison of different Routing Protocols in MANETs

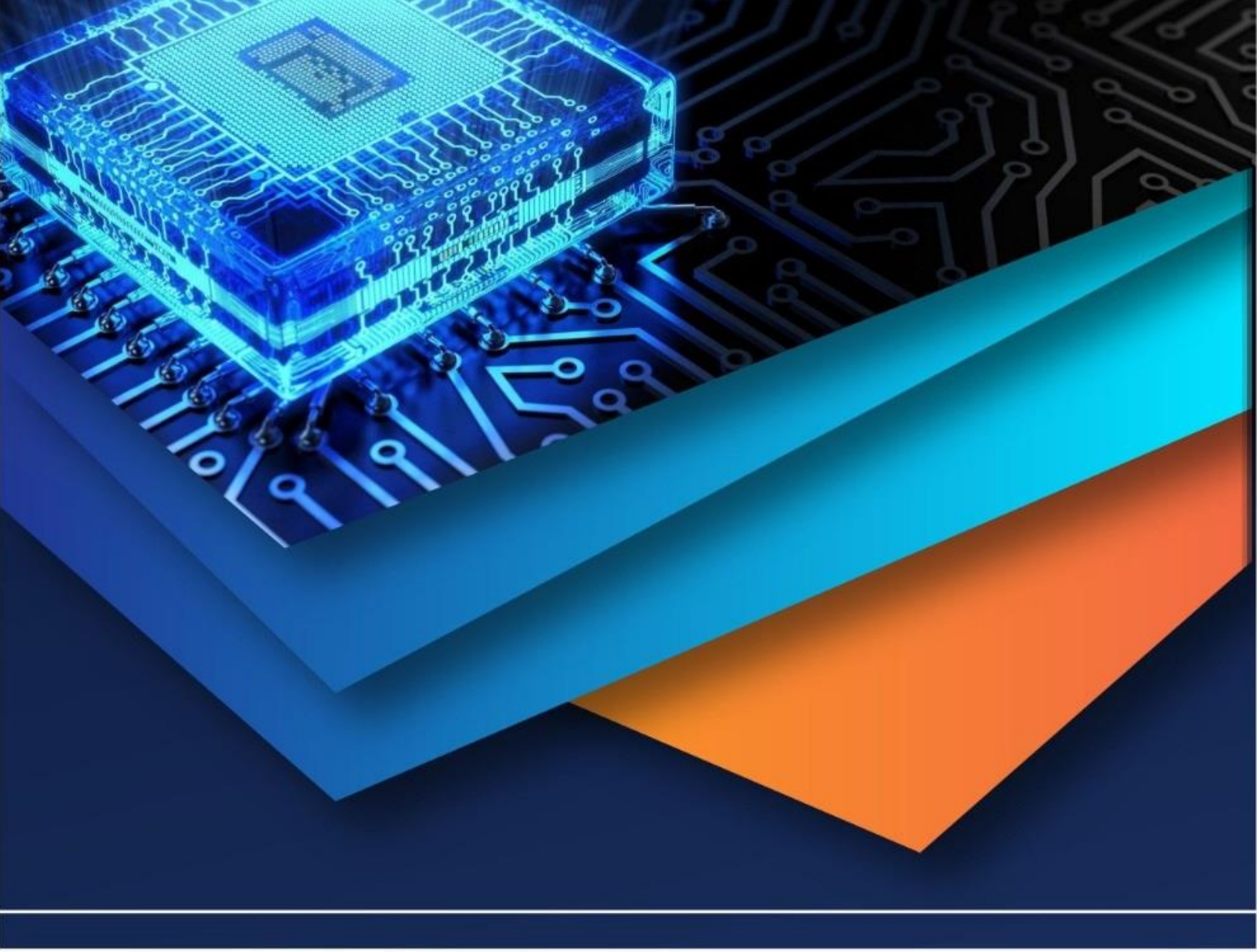
V. CONCLUSION

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. First we introduce the basics of the mobile ad hoc network. We then discuss some typical and dangerous vulnerability in the mobile ad hoc networks. Then various routing protocols are surveyed and the comparison of them is illustrated in Table 1 above. Proactive protocols are not suited to large networks as they need to maintain node entries for every single node within the routing table of any node. Periodically updating the network topology and route entries exhaust the batteries of the nodes as they always have to be active, increases the bandwidth overhead, unwanted redundant route entries. The Reactive or on demand protocols do not find the routes unless demanded hence do not update themselves to the route changes. Due to lack of awareness of the changing topology, the routes may expire after certain duration of time. Hybrid Routing Protocol is not an appropriate choice for small networks. The afore mentioned routing protocols are tactical and smart enough to deal with constraints like power consumption, low bandwidth, high error rate, and unpredictable node movements. The effectiveness of these protocols is evaluated on the basis of some quantitative performance metrics like, average end to end delay, throughput, packet delivery ratio, route acquisition time etc. The current researches have tried to emphasize on the threats, vulnerabilities and attacks, a MANET is prone to. The efforts are still going to produce much energy efficient, cheaper, and more capable mobile nodes, performance. The future of the ad hoc networks can be foreseen as a much cheaper, easily deployable, anytime, anywhere so that it may turn out to provide us with much improved network, large scale wireless network which will be able to serve a variety of applications to a variety of users.

REFRENCES

[1] JaroenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges” Journal of Computing 3(3). pp. 60-66, 2004
[2] Hung-Min Sun , Chiung-Hsun Chen ,Chih-Wen Yeh , Yao-Hsin Chen “A collaborative routing protocol against routing disruptions in MANETs,” PersUbiquitComput, vol. 17, pp 865-874, 2013
[3] P.V.Jani, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, 2002
[4] S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack.,” CIS '09 Proceedings of International Conference on Computational Intelligence and Security, vol. 02, pp. 421- 425, 2009
[5] Ritika and Malkeet Singh “Malicious Attacks and Routing Protocols in MANET: A Survey,” International Journal of Electronic and Electrical Engineering, vol. 7, Number 7 pp. 743-748 , 2014
[6] Z. J. Haas and M. R. Pearlman,” “ZRP: a hybrid framework for routing in ad hoc networks”, Ad hoc networking, pp. 221-253, 2001
[7] NavidNikaein, “HARP - HYBRID AD HOC ROUTING PROTOCOL”, 2001
[8] N. Nikaein, H. Labiod, and C. Bonnet, “DDR: distributed dynamic routing algorithm for mobile ad hoc networks,” in: First Annual Workshop on Mobile and Ad Hoc Networking and Computing, MobiHOC, pp. 19– 27, 2000
[9] Nidal Nasser and Yunfeng Chen “Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks,” IEEE International Conference on Communications, pp. 1154-115, 2007 [10] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.
[10] Yongguang Zhang and Wenke Lee, Security in Mobile Ad- Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
[11] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.
[12] JaydipSen, “A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks”, Proceedings of the 3rd International Conference on Network Security and Applications, Chennai, India, 2010, pp. 538- 537.
[13] Sonja Buchegger, Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)”, Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC’02), June 9-11, 2002, EPFL Lausanne, Switzerland, pp. 226-236.
[14] Islam Tharwat A. Halim, Hossam M. Fahmy, Ayman, M. Bahaa El-Din, Mohamed H. El-Shafey, “Agent-based Trusted On-Demand Routing Protocol for Mobile Ad-hoc Networks”, 2010 4th International Conference on Network and System Security (NSS)Sept. 1-3, 2010, pp. 255-262.
[15] Ming Yu, Mengchu Zhou, Wei Sou, “A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments”, IEEE Transactions on Vehicular Technology, vol.58, no.1, Jan.2009, pp.449-460.
[16] R. Vasudevan, SugataSanyal, “A Novel Multipath Approach to Security in Mobile and Ad Hoc Networks (MANETs)”, Proceedings of International Conference on Computers and Devices for Communication (CODEC'04), Kolkata, India, December, 2004, pp. CAN_0412_CO_F_1 to CAN_0412_CO_F_4.
[17] Gunhee Lee, Dong-kyoo Kim, JungtaekSeo, “An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks”, International Conference on Information Security and Assurance (ISA 2008), April 24-26, 2008, pp.220-225.
[18] Pallavi Sharma, AdityaTrivedi, “An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 27-29 2011, pp.307-311.
[19] AlmassianNegar, Azmi Reza, Berenji Sarah, “AIDSLK: An Anomaly Based Intrusion Detection System in Linux Kernel”, Information Systems, Technology and Management Communications in Computer and Information Science, 2009, Publisher: Springer Berlin Heidelberg, pp. 232-243.
[20] Yuxin Wei, Muqing Wu, "Intrusion detection technology based on CEGA-SVM," Third International Conference on Security and Privacy in Communications

Networks and the Workshops, (SecureComm 2007), Sept. 17-21, 2007, pp.244-249.
[21] J. Vishumathi, K.L Shunmuganathan, “A computational intelligence for evaluation of intrusion detection system”, Indian J. of Science and Technology, Jan. 2011, Issue 1, Vol. 4, pp. 40-45.
[22] Penva, Y. K, Bringas, P. G., "Integrating network misuse and anomaly prevention," 6th IEEE International Conference on Industrial Informatics, 2008. INDIN 2008, July 13-16, 2008, pp.586-591.
[23] S. Saravanakumar, Umamaheshwari, D. Jayalakshmi, R. Sugumar, “Development and implementation of artificial neural networks for intrusion detection in computer network”, Int. Journal of Computer Science and Network Security. 2010. vol. 10, no. 7, pp. 271-275.
[24] Jimmy Shun and Heidar A. Malki, “Network Intrusion Detection System Using Neural Networks”, Fourth International Conference on Natural Computation,(ICNC '08),vol.5, Oct. 18-20, 2008, pp.242-246.
[25] SampadaChavan, Khusbu Shah, Neha Dave, Sanghamitra Mukherjee, Ajith Abraham, SugataSanyal, “Adaptive Neuro-Fuzzy Intrusion Detection Systems”, IEEE International Conference on Information Technology: Coding andComputing,2004 (ITCC ’04), Proceedings of ITCC 2004, Vol. 1, April, 2004, Las Vegas, Nevada, pp. 70-74.
[26] Divyata Dal, Siby Abraham, Ajith Abraham, SugataSanyal, MukundSanglikar, “Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System”, 7th International Conference on Computer Information Systems and Industrial Management Applications, (CISIM '08), June 26-28, 2008, pp.65-70
[27] D. Dasgupta, S. Yu, F. Nino, “Recent Advances in Artificial Immune Systems: Models and Applications”, Applied Soft Computing, Elsevier, Vol. 11, March, 2011, pp.1574-1587.
[28] Jin Yang, Yi Liu, JianJun Wang, JianDong Zhang, Bin Li, "Dynamical Immunological Surveillance for Network Danger Evaluation Model," 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09), Beijing, China, Sept. 24-26, 2009, pp.1-4.
[29] F. Hosseinpour, K. Abu Bakar, A. HatamiHardoroudi, A.FarhangDareshur, "Design of a new distributed model for Intrusion Detection System based on Artificial Immune System," 2010 6th International Conference on Advanced Information Management and Service (IMS), Seoul, Korea, Nov. 30-Dec. 2, 2010, pp.378-383.
[30] MA Jie, SHI Ying-chun, ZHONG Zi-fa, LIU Xiang, "An Anomalistic Electromagnetism Signal Detection Model Based on Artificial Immune System," 2010 International Conference on Communications and Intelligence Information Security (ICCIIS),NanNing, China, Oct. 13-14, 2010,pp.256-260.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY