iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** I **Month of publication:** January 2016

DOI:

www.ijraset.com

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

Volume 4 Issue I, January 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Optimized Survey on Security Issues in Mobile Adhoc Network

Suruchi Sharma[#1], Sangeeta Monga[*2]
[#]*Electronics and Communication Department, DAV University Jalandhar, Punjab*

Abstract— Security has become a prime concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer to peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. The security solutions are therefore required to achieve both broad protection and desirable network performance. In this paper we focus on the fundamental security problem of protecting the data transmitting between two nodes in a MANET. We also identify the security issues in MANET and ongoing research in securing MANETs.

Keywords— MANET; NS2; QualNet; Routing Protocols; AODV; MAODV; VANET.

I. INTRODUCTION

A mobile ad hoc network, generally known as MANET is relatively new communication paradigm. MANET has received spectacular consideration because of their self-configuration and self-maintenance. We are moving from the traditional wired communications to wireless communications. Early research assumed a friendly and cooperative environment of wireless network. As a result they focused on problems such as wireless channel access and multi hop routing. But security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Although mobile ad hoc networks have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks as described by Basagni et.al (2010).

MANETs lack central administration and prior organization, so the security issues are different and thus requires different security mechanisms than in conventional networks. Wireless links in MANETs make them more prone to attacks. It is easy for hackers to attack these networks and thus gain access to confidential information. They can also directly attack the network to delete messages, add malicious messages, or masquerade as a node. These challenges include open network architecture, shared wireless medium, demanding resource constraints, and highly dynamic network topology. The objective of this paper is to study the work done by different researchers in this field of MANET.

II. LITERATURE SURVEY

A. The solution of Black hole attack that could happen easily in AODV protocol of MANETs, which is known to be an important on-demand protocol, was given by Deng et.al (2002) by continuing a reply message to come from intermediate nodes and have a check on this process which further leads to a great increase in routing overheads.

B. Yang et.al (2004) discussed various challenges offered by the Routing Protocols. They proposed a Multi fence security solution to the attacks and challenges that achieves both broad protection and desirable network performance. In addition, they also entitled the secure ad hoc routing protocols to enhance the existing protocols, such as AODV and DSR, by preferring proactive approach, with security extensions. Therefore, the solution achieves all the three functional elements of prevention, detection and reaction in order to guard the entire system.

C. Zhao et.al (1999) gave a new algorithm and made a qualitative comparison with MAODV on various parameters. The author suggested that gateway loading is not considered in existing MAODV. He suggested a few modifications in existing algorithms that overcomes many of the drawbacks of MAODV and shows that MAODV is better than other algorithms, at low speeds it achieves 95% packet delivery and at high speeds it decreases to 50%.

D. The features of MANET are provided in the paper presented by Sheikh et.al (2010) which need more secure operations in MANET that current routing protocols do not focus on. This paper explores security issues in MANETs and therby propose some methods of secure multiparty computations (SMC) to achieve the security. Also, three further types of solutions such as Cryptosystem, Randomization methods and anonymization methods are available in this paper. These methods provide privacy-preservation during computation process.

E. Wireless security studies by C. Hu et.al (2004) have discussed the properties of security, such as confidentiality, integrity, authentication, availability, fairness, anonymity, non-source-based routing. They suggested the improved algorithms to solve the problem of hijacking, loss of security and lack of source control over route length which can overall improve the performance of the wireless system.

F. Chang et.al (2010) described a security analysis of MANET and found that the security of Mobile Ad hoc Network (MANET) is more rigorous than the traditional networks. The author proposed MANET architecture design to provide specific framework for the design of secure MANET network in reference of OSI reference model that concluded confidential, reliable and complete data transmission in a highly poor environment.

G. The routing rule and transmission scheme were proposed by Wu and Liaw (2015) which are not only satisfied with the security properties of previous scheme but also satisfy the efficiency property. The efficiency analysis was based on the comparison between the scheme provided by Boukerche and Wu et al.'s scheme and the results showed that the scheme proposed in this paper is good for both security and efficiency purpose.

H. The security threats an Ad hoc network faces and the security objectives that need to be achieved are enlisted by Zhou and Haas (1999). The main focus of their work is to secure routing and establish a secure key management service in an Ad hoc networking environment. This work is supported by ARPA/RADC grant, AFOSR grant, DARPA and Air force research laboratory. They suggested a prototype of the key management service, which shows its feasibility to build a highly available and highly secure key management service.

I. Karlsson et.al (2012) gave the overall idea of several routing protocols used in several past years and also enlightens the criteria of selecting a routing protocol. Due to strong cryptographic protection of routing messages, attacks such as modification, impersonation, and fabrication are effectively eliminated by using security extensions for some MANET routing protocols of DSR, DSDV and ZRP is concluded in this paper.

J. Nodes perform Neighbour position verification (Npv) to know the position of nodes which are detected by the priori trustworthy nodes. A distributed solution for Npv when the priori trustworthy nodes are absent has been presented by Ramojeerao et.al (2014). The Simulation results authenticate that any node in a mobile ad hoc network confirm the position of its communication neighbours without relying on a priori trustworthy nodes.

K. Stajano and Anderson (1999) have presented a resurrecting duckling security policy model of secure transient association. The described the new attacks such as sleep deprivation torture and limitations on the acceptable primitives for cryptographic protocols. They studied the main security issues which arise in ad hoc wireless network of mobile devices. Hence, Resurrecting duckling security policy provides a secure use of device with multiple users.

L. Hu and Perrig (2004) review attacks on Ad hoc networks and discuss current approaches for establishing cryptographic keys in Ad hoc networks. They described the state of research in secure Ad hoc routing protocols and its research challenges. Various possible ways are discussed in order to avoid routing misbehavior. Cryptographic key approach used results in a strong security and high network performance.

M. Secured routing technique of MANET was analysed by Subramaniam et.al (2013). The main aim was to concentrate on a design of a more secure routing protocol for Ad hoc networks. A qualitative comparison was made between several routing protocols among their accuracy, speed and cost. Using GloMoSim network simulator, activities of various routing protocols were analysed for their throughputs, energy consumption and collision. An Endaira algorithm was presented which detects and removes the availability of black/grey hole attack in the ad hoc network and as a result provides more security for route discovery in Mobile Ad hoc network.

N. The fundamental issues and analyses key research problems of MANET have been presented by Sun (2001). He described the background information of MANET, including the MANET concept, features, current status, and application areas. The main challenges of MANET are also discussed that leads to the analysis of relevant kernel barrier. He provided a fault-tolerant routing scheme in which overhead occurs and this result in increasing the reliability and security of the target routing algorithm.

O. Cho et.al (2011), have analyzed existing trust management schemes in MANETs to provide trust network protocol designers with multiple perspectives. They presented trust properties that were observed in developing trust metrics to meet the requirements and goals of the targeted system. It is observed that considering an individual node in the system can be easier to defend from malicious attacks which results in reduction of errors.

P. Li and Wang (2007) discussed the various routing protocols and their challenges in VANETs. It discusses the performance of a routing protocol in VANETs depends heavily on the mobility model, the driving environment, the vehicular density. VANET and

MANET share the same principle and the results showed that most ad hoc routing protocols in VANET suffer from highly dynamic nature of node mobility.

Q. Classification of network layer attacks has been presented by Nadeem (2003). He has reviewed the point detection algorithms proposed to secure MANETs from specific network layer attacks. The paper introduces the main categories of intrusion detection systems and describes the challenges of implementing IDSs in MANETs and their architectures. It has been observed that by enabling robust protection mechanism we can infer and detect new intrusive activities and no introduction of new vulnerabilities into the system takes place.

R. Toubiana and Labiod (2008) have contributed the solution named Adaptive Secured Multipath for Ad hoc networks (ASMA) to provide efficient security management. The enhancement of ASMA flexibility was done to support another multipath routing protocol: AOMDV. They have compared the new combination ASMA-AOMDV to the AOMDV multipath routing protocol. ASMA-AOMDV outperforms AOMDV using NS2 and achieves packet delivery ratio lower than the ones of AOMDV. The traffic load generated by full multipath routing protocols AOMDV causes performance degradation and AOMDV route acquisition time is higher than ASMA-AOMDV. Hence ASMA provides security and acceptable performance.

S. A new level of routing security protocol ORZEF(An Optimized Routing using Zone to Establish Security in MANET using Friendly Multipath) has been proposed by Thandavarayan et.al (2012) which shares secret key for data transmission. The comparison among ORZEF, FACES, ZRP using QualNet simulator shows that ORZEF scheme provides an efficient approach towards security along with easier detection of the malicious nodes in the mobile ad hoc network. Moreover the power is also effectively utilized.

T. Perkins and Royer (1999) described the security-sensitive applications of ad hoc networks which require high degree of security. Ad hoc networks are inherently vulnerable to security attacks and security mechanisms are indispensable for ad hoc networks. This paper analyzes the security threats, understands the security requirements for ad hoc networks, identifies existing techniques and proposes new mechanisms to secure Ad hoc Networks.

U. Komai and Yuka (2015) proposed the filling area (FA) method to efficiently process kNN (kth nearest neighbor) queries in the MANETs. The FA method achieves low overhead in query processing by reducing a search area. In the FA method, data items remain at nodes near the locations with which the items are associated, and nodes cache data items whose locations are near their own so that the query issuer retrieves kNNs from nearby nodes. Through extensive simulations, we verify that our proposed approach achieves low overhead and high accuracy of the query result.

V. Whittenton, Nathan, and Theodore Berger (2013) presented WaSPNet (Waterborne Surveillance and Protection Network) aimed at providing a solution to the complex problem of maritime security. It comprises a swarm of network members, each configured as necessary in terms of sensor packages, mobility requirements and network capabilities to provide for information gathering and dissemination. A secure mobile ad hoc network of multiple unmanned maritime sensor equipped platforms meshed with existing fixed sensor networks can provide operators and decision makers with real-time eyes and ears on the scene. Initial operational experiments have validated this concept by integrating multiple sensing modalities through a mesh capable extended Ethernet WAN consisting of varied types of communication links. Extending this network across organizational boundaries will enhance decision making capabilities, enabling immediate responses to environmental, criminal, safety and security threats.

W. He and Liang (2012) investigated the online scenario where data collection requests arrive progressively, and the data collection process is modelled as an M/G/1/c-NJN queuing system, where NJN stands for nearest-job-next, a simple and intuitive service discipline. Based on this model, the performance of data collection is evaluated through both theoretical analysis and extensive simulation. The NJN discipline is further extended by considering the possibility of requests combination (NJNC). The simulation results validate our analytical models and give more insights when comparing with the first-come-first-serve (FCFS) discipline. In contrast to the conventional wisdom of the starvation problem, we reveal that NJN and NJNC have a better performance than FCFS, in both the average and more importantly the worst cases, which gives the much needed assurance to adopt NJN and NJNC in the design of more sophisticated data collection schemes for mobile elements in wireless ad hoc sensor networks, as well as many other similar scheduling application scenarios.

X. Balasubramaniyan, R., and M. Chandrasekaran (2013) proposed a Fuzzy Relevance-based Cluster head selection Algorithm (FRCA) to solve problems found in existing wireless mobile ad hoc sensor networks, such as the node distribution found in dynamic properties due to mobility and flat structures and disturbance of the cluster formation. The proposed mechanism uses fuzzy relevance to select the cluster head for clustering in wireless mobile ad hoc sensor networks. In the simulation implemented on the NS-2 simulator, the proposed FRCA is compared with algorithms such as the Cluster-based Routing Protocol (CBRP), the

Weighted-based Adaptive Clustering Algorithm (WACA), and the Scenario-based Clustering Algorithm for Mobile ad hoc networks (SCAM). The simulation results showed that the proposed FRCA achieves better performance than other existing mechanisms.

Y. Hu and Lingxiao (2014) established a model of mobile ad-hoc network using UAVs. And this UAVs network can be also called a special military mobile ad-hoc network, based on which, this paper adopted feasible performance metrics modelling method of route optimization problem. Then the above route programming theory developed into running visible software by Visual C++. Genetic Algorithm (GA) is the core of this new software. Finally, the running result verified this route planning's solution is effective in scene of battlefield by this new visible software.

III. CONCLUSIONS

MANET is a growing field in the wireless communication system having its own pros and cons. Besides this it has many features which could help in the communication field. In this survey paper, we have analysed the security threats an ad hoc network faces and the security objectives that need to be achieved. The main issue in MANET is to secure it from numerous attacks. We have taken into consideration many scenarios to study the security protocols used for securing the databases in MANET and a lot more research is to be done in this field.

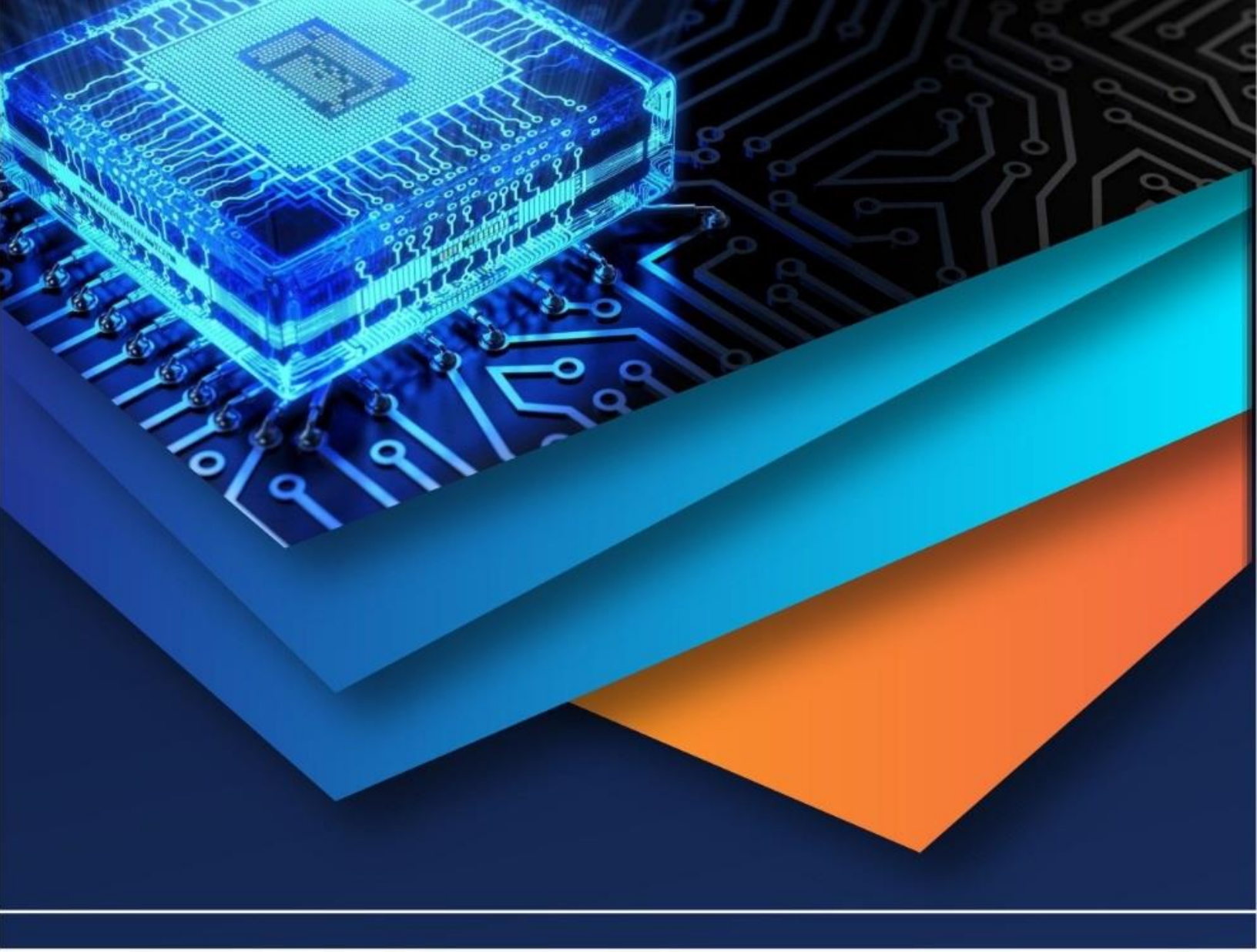
IV. ACKNOWLEDGMENT

I would like to thank sincerely to my guide Sangeeta Monga who gave her invaluable guidance, constant assistance, support, endurance and constructive suggestions for the betterment of the technical seminar. I also wish to thank all the staff members of electronics and communication department for helping directly or indirectly in completing this work successfully. Finally I am thankful to my parents and friends for their moral and material support throughout the course and in helping me finalize this survey paper.

REFERENCES

[1] Adnan Nadeem, “A survey of MANET intrusion, detection and prevention approaches for network layer attacks”, IEEE Communications surveys and tutorials, 2013, Vol.15, Issue 4, pp.2027-2045.
[2] B. Praveen Kumar, P. Chandra Sekhar, N. Papanna and B. Bharath Bhushan, “A Survey on MANET security challenges and routing protocols”, Int. J. Computer Technology and applications, 2013, Vol. 4, Issue 2, pp. 248-256
[3] Balasubramaniyan, R., and M. Chandrasekaran, "A new fuzzy based clustering algorithm for wireless mobile Ad-Hoc sensor networks", Computer Communication and Informatics (ICCCI), 2013 International Conference on, IEEE.
[4] C. Perkins and E. Royer, “Ad hoc on-demand distance vector routing”, IEEE WMCSA, 1999, pp.90.
[5] F. Stajano and R. Anderson,” The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks”, Security Protocols, 7th International Workshop, IEEE, LNCS, Springer-Verlag, 1999, pp.22-26.
[6] Gokulnath Thandavarayan, Sangeetha K and Selvaraj Seerangan, “ORZEF: An optimized routing using zone to establish security in MANET using multipath and friendly based Adhoc routing”,Proceedings of the International Conference on Pattern recognition, informatics and medical engineering, IEEE, 2012, pp. 221-224.
[7] Gowsiga Subramaniam, Senthil Kumar Ponnusamy and Muneeswari A, “An Analysis of Secured Routing technique in mobile Adhoc networks”, IJC, 2013, Vol. 2, Issue 1, pp. 21-30.
[8] He and Liang, "Evaluating service disciplines for mobile elements in wireless ad hoc sensor networks", INFOCOM, 2012 Proceedings IEEE. IEEE, 2012.
[9] Hongmei Deng, Wei Li and Dharma P. Agrawal, “Routing Security in wireless Adhoc networks”, Telecommunication network security, IEEE Communications Magazine, 2002, pp.46-55.
[10] Hu and Lingxia, "Optimal path planning of mobile ad-hoc sensor network using unmanned aerial vehicles'(UAVs')", Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on. IEEE, 2014.
[11] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Adhoc Networks”, Proceedings of the Ninth International Conference on Network Protocols, IEEE, 2001 pp.1092-1658.
[12] Jin-Hee Chao, Ananthram Swami and Ing-Ray Chen, “A survey on trust management for mobile Adhoc networks”, IEEE Communications Survey and tutorials, 2011, Vol. 13, Issue 14, pp. 562-583.
[13] Jonny Karlsson, Laurence S. Dooley and Goran Pulkkis, “Routing security in mobile Adhoc networks”, Issues in Informing Science and information Technology, 2012, Vol. 9, pp. 369-383.
[14] Jun-Zhao Sun, “Mobile Adhoc Networking: An essential technology for pervasive computing”, IEEE, 2001, pp. 316-321.
[15] Komai and Yuka, "Nearest Neighbor Search for Location-Dependent Sensor Data in MANETs”, IEEE 3, 2015, pp. 942-954.
[16] Li Shi-Chang,Yang Hao and Zhu Qing-Sheng, “Research on MANET Security Architecture Design”, International Conference on Signal Acquisition and Processing, IEEE, 2010, pp. 90-93.
[17] Lidong Zhou and Zygmunt J. Haas, “Security Adhoc networks”, Special issue on network security, IEEE Network, 1999, pp.24-30.
[18] Mazda Salmanian, Li Pan, Jiangxin Hu and Ming Li, “On the efficiency of establishing and maintaining security associations in tactical MANETs in group formation”, Cyber security and network operations, The Military communications conference, Track 3, IEEE, 2011, pp. 1176-1182.
[19] P. Ramojeerao, G. Raju and K.T.V. Subbarao, “A distributed solution for Npv in mobile Adhoc networks to verify the position of communication neighbours”, International Journal of Science engineering and Advance Technology(IJSEAT), 2014, Vol. 2, Issue 12, pp. 1021-1024.

[20] Rashid Sheikh, Mahakal Singh Chandel and Durgesh Kumar Mishra, "Security Issues in MANET: A Review", IEEE, 2010, pp.124-128.
[21] Shubham Joshi and Dr. Durgesh Kumar Mishra, "A survey on threats in routing in routing security in MANET for trust management using SMC protocols", WOCN conference, 2012, pp.1-6.
[22] Stefano Basagni, Marco Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Adhoc Networking", IEEE, 2010, pp.255-373.
[23] Vincent Toubiana and Honda Labiod, "Towards a flexible security management solution for dynamic MANETs", Ecole Nationale Superieure des Telecommunication(ENST), IEEE, 2008, pp. 963-966.
[24] Wei-Chen Wu and Horng-Twu Liaw, "A study on High Secure and efficient MANET Routing Scheme", Hindawi publishing Corporation, 2015, Article No.365863.
[25] Whittenton, Nathan, and Theodore Berger,"Mobile ad hoc network of waterborne sensors for enhanced maritime security", Oceans-San Diego, IEEE, 2013.
[26] Yih-Chun Hu and Adrian Perrig," A survey of secure wireless Adhoc routing", IEEE Security and Privacy, ICE, 2004, pp. 28-39.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY