iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IX **Month of publication:** September 2018

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

Adaptive Security Model to Prevent Intentional Power Draining In MANET

Sukriti Bhatnagar[1], Praveen Kumar Gautam[2]
[1]*Research Scholar-CSE,* [2]*Asst. Professor-CSE, Truba College of Engineering and Technology, Indore*

Abstract: ***MANET is vulnerable to environment, which form weak security system. When comparing with wired network, this network is more vulnerable because of compromised nodes. Security is very important solution for MANET. The main aim of this work is to prevent MANET from power draining using adaptive security model and also related survey on various kinds of attack which affect behavior of MANET. In this work detection of attack using the medical examination survey will be performed, where work will be sequenced depending on medical diagnosis.***
Keywords: MANET, detection algorithm, power draining attacks, security

I. INTRODUCTION

MANET stands for Mobile Ad Hoc Network, and due to the emerging technology it has become a prevailing field for research because of challenges on relevant protocols. This technology helps in communicating without and physical channel, no matters any geographical location. That is the reason, this network is called as infrastructure less network. With the growth of powerful, small and cheaper device form MANET as a fastest enhancing network.

Ad hoc is a self organizing network which is adaptive to supportive network operations. Presence of other devices are detected in mobile ad hoc network and other necessary set ups are facilitated for data communication and sharing services. Connections are maintained in network with supple addition and deletion of device from networks. Applications of MANET are: static networks, large-scale ranging, dynamic networks and other sources. Application environment movement from infrastructure to ad hoc context deals with new sources and services with generation of different environments inclusion of:

1) Medical Services
2) Sensor networks
3) Personal area network
4) Military Battlefield

Security is very important solution for MANET, it is most importantly used for the selection of sensitive applications. But important is to meet all the goals with mentioned challenges in problem statement sections. When comparing with wired network, this network is more vulnerable because of compromised nodes, limited physical security and lack of centralized management, due to these vulnerabilities MANET is more inclined towards malicious attacks. The main aim of this work is to prevent MANET from power draining using adaptive security model and also related survey on various kinds of attack which affect behavior of MANET.

MANET is vulnerable to environment, which form weak security system. Vulnerability leads to unauthorized manipulation of data because of not identifying user's identity by system before any access to data. Its vulnerability is more than wired network. Some vulnerability is:

a) Lack of Centralized management
b) Resource availability
c) Scalability
d) Cooperativeness
e) Dynamic topology
f) Limited power supply

II. RELATED WORK

A. *Study of Base Paper*

A.Naveena et al. In[1] explained about low power ad hoc system, which is a challenging prospect for secure Ad Hoc systems. The devices which are forced to utilize resources were the cause for easily unauthorized damage to limited operations. Author proposed an energy efficient routing protocol to achieve low power MANETs. Key generations where reduced by data transfer and routing anonymous with achieving overheads for control packets. Public key generations are reduced in this work for the purpose of

security and energy efficiency. Performance of the work is compared with other routing protocols like SADR and AASR. Better energy efficiency is achieved in proposed work, depending on simulation result.

B. Related Work

Yanchao Zhang et al. In [2] introduces about ad-hoc network which self maintained network and dynamically organizes topology without any need of resources. Secure protocols are proposed for privacy but performance efficiency can not be maintained. A routing protocol for privacy maintenance of node is implemented and also prevent traffic analysis and other attacks. Attacks here, are classified as passive and active attack. In this paper author considered and analyzed active and passive attack for secure communication.

Haiying shen et al. In[3] proposed a location-based Anonymous routing protocol which is efficient to protect location anonymity. This protocol is abstracted as ALERT. This protocol works as, source and destination partition of network and does not provides authentication to node. Networks are organized into zones in this protocol. Related groups are organized in networks in this protocol. If any node in the group is dishonest then the complete group is considered as dishonest.

Wei liu et al. In [4] proposed an AASR protocol for the efficient anonymity where group signatures and key encryption maintains network anonymity for achieving on-demand security. Deficiency in cryptographic is the reason for imbalance energy. With less delay time most of the protocols performs secure routing. In terms of efficiency of energy these protocols are limited.

A. Boukerche et al. In[5] focuses on reducing energy consumption by generating key operations and validations. For packet decryption, a private key and shared session key are represented between nodes. If shared session is already there, then no need to generate new session key. Operations for generating public keys are reduced by anonymous public key. In most of the anonymous routing protocol, control packets are used for route discovery. In this work no pre process approach is required. More energy is consumed by control packets. No any prior control packets are organized here, so energy can be saved in this work.

III. PROBLEM STATEMENT

Problem defines the detection of attack, because detecting attack in network is difficult. Many different types of attacks are involved in the existing work.

Problem definition defines various types of attacks and these attacks are categorized into two types:

1) *Active Attacks:* Due to malicious nodes, active attacks are performed which consumes energy cost to perform attacks. Modification of data and creation of false data is involved in this attack. Active attack is classified as internal attack or external attack. Where, external attacks are due to the external node which is not the member of network. Whereas, internal attack is due to the compromising of node belonging to that network. Here, attacker is already a part of the network. In terms of detection of attack, internal attack is more strong and not easy to detect than external attack. Active attacks include following attacks as:

a) Black hole attack
b) wormhole attack
c) Sinkhole attack
d) Gray-hole attack
e) Replay attack
f) Flooding
g) Spoofing attack
h) Jamming
i) Denial-of-Service
j) Man-in-the middle

2) *Passive Attacks:* Passive attack does not interrupt proper network operations. Without any alteration snooper exchange data in network. Confidentiality can be loose if attacker interpret the gathered data by snooping. These attacks are difficult to detect because the networks operations does not affect itself. Some of the passive attacks are:

1) Traffic monitoring
2) Eavesdropping
3) Traffic Analysis
4) Syn flooding

IV. PROPOSED SOLUTION

Solution proposed from the following issue observes the detection of attack. Different types of attacks can be detected in the proposed solution. For example, a survey is made on medical examination, which concluded that, if any patient is suffering from malaria then his/her hemoglobin is less. Doctors diagnosed this issue of low hemoglobin in patient due to the suffering of malaria and if patient suffering from dengue than is diagnosed and identified that platelets are less.

This type of examples are related to our work, because here, diagnosis is done to identify the mitigate approach which detects attacks, because it is difficult to detect which attack happened in network and which node is the attacker node. So, the proposed work achieves the issue of detecting the attack in MANET network.

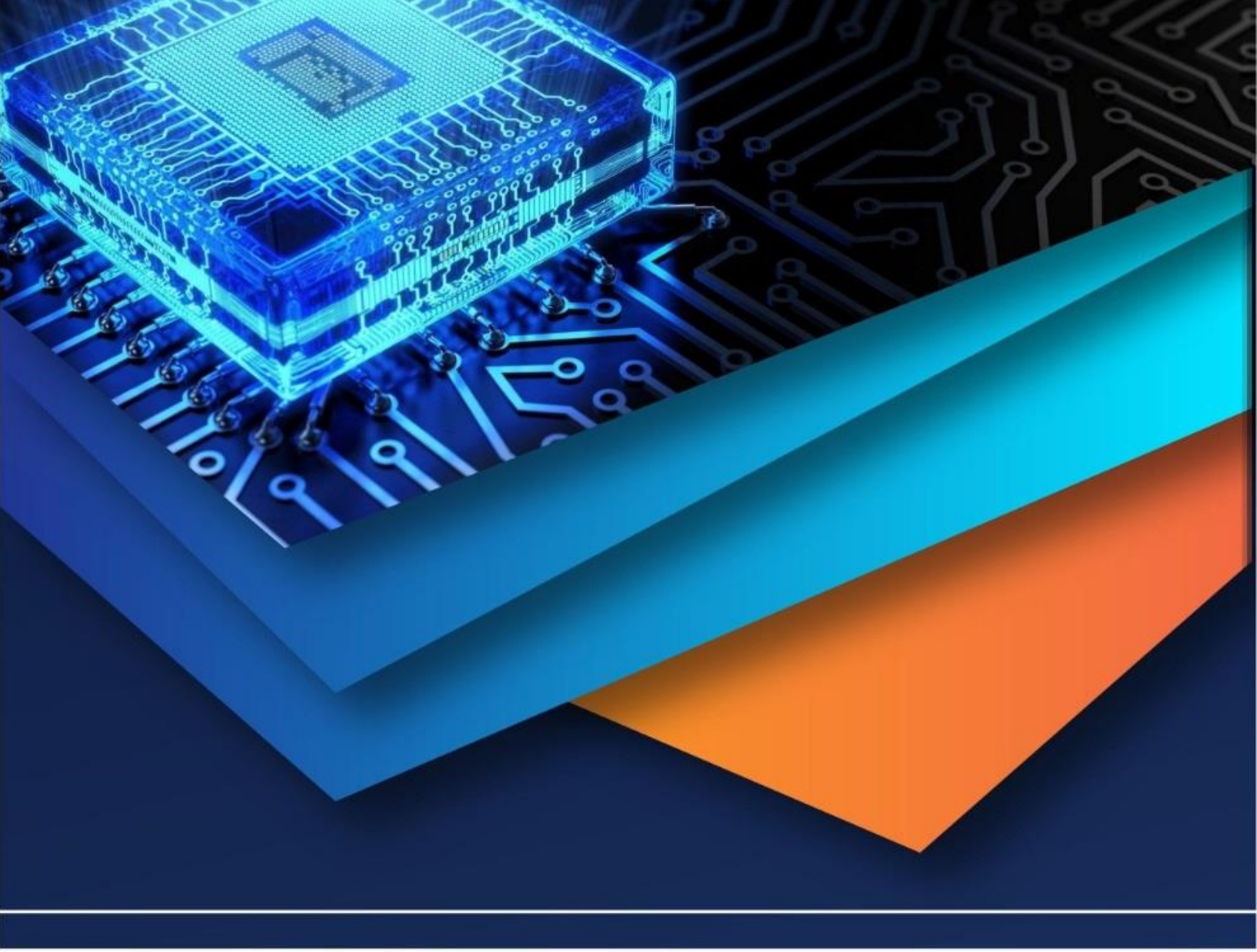
Detection of vampire attack is more difficult when comparing with other attacks. Whereas, DDoS attack is little bit less than vampire attack in terms of detection and moving on to other attacks, then sequence started. To overcome this issue, survey is made in our work for the detection of attack using the medical examination survey, where work will be sequenced depending on medical diagnose and is explained above with example.

V. CONCLUSION

This paper research about the detection of attack and is concluded that various types of attacks are there and with different behavior, some attacks are easy to detect but some attacks can not be detected easily. In MANET network, work will be performed on the basis of challenging requirements. Power draining of node is the challenging issue in MANET network.

REFERENCES

[1] A.Naveena, Dr. K.Rama Linga Reddy, “Lightweight Energy Proficient Anonymous Routing for Low-power MANET”. 2017 IEEE 7th International Advance Computing Conference
[2] Yanchao Zhang; Wei Liu; Wenjing Lou; “Anonymous communications in mobile ad hoc networks “INFOCOM 2005. 24th Annual Joint
[3] Haiying shen, member, and lianyu zhao, “alert: an anonymous location-based efficient routing protocol in manets”, IEEE transactions on mobile computing, vol. 12, no. 6, june 2013
[4] wei liu, member, and ming yu, “aasr: authenticated anonymous secure routing for manets in adversarial environments”, IEEE transactions on vehicular technology, vol. 63, no. 9, November 2014
[5] A. Boukerche, K. EI-Khatib, L. Xu, and L. Korba. "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Network", The 29th Annual IEEE International Conference on Local Computer Networks, Tampa, Florida, USA, 2004
[6] K. E. Defrawy and G. Tsudik, “ALARM: Anonymous location-aided routing in suspicious MANETs,” IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, Sep. 201
[7] J. Kong, and X. Hong, “ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks,” in Proc. 4Th International Symposium on Mobile Ad Hoc Networking & Computing, New York, 2003, pp. 291-302
[8] Q. Yang, H. Dijiang, and K. Vinayak, “OLAR: On-demand Lightweight Anonymous Routing in MANETs,” in Proc. 4th International Conference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.
[9] Goldwasser, S. S Micali and C. Rackoff, “Knowledge Complexity of Interactive Proof Systems”, Proceedings of STOC 1985, PP. 291-304
[10] D. Johnson, and A. Menezes, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Technical Report CORR 99-34, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 1999.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY