A SURVEY ON ENERGY EFFICIENT USAGE OF INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS

[1]N.Venkateswaran, [2]Dr. K.Umadevi, [3]Dr. A. ViswaBharathy, [4]Dr. R. Jegadeesan

[1]Research Scholar, Anna University, [2]Professor, [3,4]Associate Professor
[1]Department of Computer Science and Engineering
[2]Department of Electronics and Communication Engineering
[3,4]Department of Computer Science and Engineering

Abstract: Mobile Adhoc Network (MANET) is a cluster of wireless movable nodes and are self-created and self-organized, in which all the nodes move and communicate with each other in the network through radio energy without any centralized control and base stations. In this network infrastructure, every node is independent. Thus, due to its original nature of mobility, network changes its frequency, so it's a challenging task to provide secure energy efficient routing in MANATs. Intrusion Detection Systems (IDS) are implemented in MANETs to monitor the activities of nodes, to discover any interruption in a susceptible network. A probabilistic model projected that makes utilization of participation involving IDSs among neighborhood nodes to moderate their dynamic time. In this Literature paper, first gives a quick survey of different types of IDS designed to protect attacks in MANET. Then, focus on intrusion detection capabilities for MANETs.

***IndexTerms*: MANETs, Intrusion detection system, Ad hoc networks, intrusion detection, energy efficiency.**

I. INTRODUCTION
II.

MANET is infrastructure less, highly capable and speedy deployable wireless based network technology. MANAT is self-configured and shortly used the network, and their routing decisions, data operations and data transmissions will be carried out by the node itself. MANET is adaptive networks that can be generated and ingenerated without the need of any federal administration. These extensive essential features help MANET very much crucial in the regions of real-world applications where the fast and irregular change in the topology occurs.

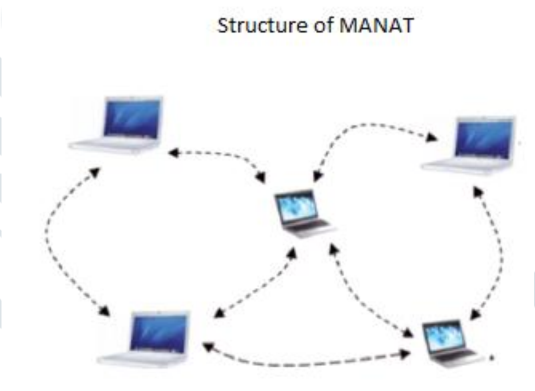

Figure: 1 Structure of MANAT

In the mobile network architecture, a node will play as a router and a host to broadcast the data to the target node, and it may connect and depart the network dynamically. In this network, no centralised control or pre-existing communications exists. MANETs are unexciting to a range of security attacks. So it is massively desirable for MANETs to make use of secure routing techniques and protocols to ensure network privacy, reliability, legitimacy and accessibility. The different types of security solutions are available that works well for wired networks and will not fit into the MANETs. The potential usage of secure routing protocols in the mobile system, the effect of several security attacks abridged.

II. INTRUSION DETECTION SYSTEM (IDS)

An ID is competent to detect the intrusions and alerting the administrator of the system about the signs of possible interventions. It provides information against any lack of confidentiality, integrity and availability of the enterprise's cerebral resources.
Due to rapid growth and trends in global networks, intrusion detection is the process applied to discover intrusions. An ID technique is implemented to sense all types of vicious attacks in the network traffic and an environment like computer usage that will not be detected by a conservative security firewall. The attacks which include data ambitious on applications, network attacks against vulnerable services, some of the host-based attacks are fake credential logins, privilege escalation, the right of entry to sensitive files and malicious program. Security is very much essential for the users to save their systems from external unprivileged resources. In the security aspect, the firewall model is one of the present protection techniques are implemented to protect the network. ID techniques are used in web-related system activities such as medical related web applications, credit card frauds determination and an Insurance agency system. [12].
IDS are a mechanism or software application that monitors the entire network traffic or system for dangerous activities or strategy destruction and generates reports to base stations. Different types of IDS are represented such as:

2.1 ACTIVE INTRUSION DETECTION SYSTEM (AIDS)

AIDS system is configured to block suspected attacks in advancement automatically, without any involvement of the user.

2.2 PASSIVE INTRUSION DETECTION SYSTEM (PIDS)

PIDS system is configured only to analyze and monitor the network traffic activity and on the alert about potential exposure and attacks to a user.

2.3 HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)

HIDS was earliest intrusion detection software designed for mainframe computers to observe the unusual behaviour in target systems. Primary responsibilities carried by HIDS are to monitoring the state, dynamic behavior, control the intrusion attempts on critical systems and inspect the packets on the network. HIDS investigate and detect the recourses availability, and if changes have occurred on the web and alert messages sent to the system administrator. It can also supervise all the individual workstations on which the software agent has installed. If changes have occurred on the network and alert messages sent to the system administrator [13].

2.4 NETWORK-BASED INTRUSION DETECTION SYSTEM (NIDS)

NIDS consists of a network antenna with a Network Interface Card (NIC) and independent board interface. The IDS is placed along a network sector or edge to observe all the traffic on the network segment. NIC systems designed to collect the necessary information from the network source fluency than each separate host. The NIDS inspect the network-based attacks; while packets transmitted around the web. The ease of the monitors decreases the chance that a challenger will be able to locate it and cancel its capabilities without the efforts. Network Node IDS (NNIDS) agents have installed the software on an individual workstation within the network protected environment. Depending upon the functionality, network-based IDS divided into two types. They are Pattern matching IDS and Statistical anomaly IDS.

2.5 APPLICATION BASED INTRUSION DETECTION SYSTEM (AIDS)

AIDS that analysis the actions are transpired within a software application. The most regular data source for AIDS is the general application’s transaction log file. AIDS monitor the interaction between user and application and AIDS is capable of operating when incoming data is encrypted.

2.6 KNOWLEDGE BASED INTRUSION DETECTION SYSTEM (KIDS):

KIDS used to generate proof of an intrusion and attacks that stored in the database, and the database referred when a malicious attack or similar kind of state arises since each intervention leaves the path behind and these paths involved and are implemented to identify and avoid the same offences in future. KIDS designed to determine intrusion attempts.

2.7 BEHAVIOR BASED INTRUSION DETECTION SYSTEM (BIDS):

BIDS provides capabilities, for controlling of the system are monitored, and it assumes intrusion if there are any changes from the usual or expected behavior of the system. When a variation occurs, an alarm generated. In other words, anything that does not correspond to a previously learned response considered. The problem with this system is the high fake alarm rate, during the learning phase, the entire range of the behavior of an information system may not cover.

III. LITERATURE SURVEY

3.1: In SCAN: self-organized network layer security in MANETs, each node autonomously detects any malicious nodes in its neighborhood and observes the routing path and packet forwarding performance of its neighbours. While each node diagonally sees its neighbours separately, all the nodes in a local community join forces with each other to ultimately convict a guarded node. This will implemented and achieved by a distributed consensus mechanism, in which a node sentenced only when its multiple neighbours have reached such a consensus. Once its neighbour’s offender a malevolent node, the network reacts by depriving its right to use the network system [2]. As per results, SCAN can detect more than 90% of the malicious nodes.

3.2 MOBILE AGENTS IDS SYSTEMS:

Autonomous Agents for Intrusion Detection (AAFID) task to make use of multiple layers of agents controlled in a hierarchical framework with each layer performing a group of intrusion detection tasks. DIDMA organise and performs decentralised data examination using mobile agents that make it more scalable. In this article, different layers of works in combination and if these layers suspect an intruder, immediate action taken. Yinan li and ZhihongQian has proposed MANET based model, an Agent-based Intrusion Detection Model which generates a cluster-head-centred vertebra network by using a type of decision mode of joint detection implemented in the middle of cluster heads and take part in a ballot in partial cluster heads to perform the total network intrusion detection [3].

3.3 SELF ORGANISED MAPS BASED IDS

IDS are run based on artificial neural network model such as Self-Organizing Map (SOM) depends on input patterns. This article proposed a model that handles different types of malware attacks and their difference of revealing approach based on self-organized map model. The strategy focused and aids at increasing the efficiency of a high level of detection rate as well as decreasing the False alarm rate [4].

3.4 CLASSIFICATION BASED IDS

Intrusion detection techniques habitually used as a continuous line of protection in MANETs. Sequentially to bring out the performance, they assess five supervised [5] categorization of algorithms for intrusion exposures method. All the algorithms measured their performance on a dataset and demonstrated in which consist of altered traffic conditions and moveable structure for various attacks. How categorization algorithms performance based on the difficulty cost matrix. As a result, inspect how the use of reliable versus weighted cost matrices influences the classifier performance. Accordingly, we enlarge the chronological cross support system, so that not all the types of attacks determination essentially be current transversely all folds.

3.5 Novel Honeypot based approach (NHPBA)

In MANATs, black hole attacker nodes isolated by adapting NHPBA approach [6]. This approach is accountable for reducing the overhead of network traffic and packet dropping ratio. In this article, an original black hole attack detection technique proposed, which mainly uses Cumulative Sum concepts to ensure changes in the sequence number of AODV protocol. Main advantages are the detection of selective packet dropping nodes in the MANETs, decrease the false alarm performance and also include the responsibility of minimizing false positive rates.

3.6 Fuzzy Based IDS

IDS and association with fuzzy logic approach were proposed to detect and recognize the types of malicious attacks [7]. In this article, suggested techniques are strong enough to understand all kinds of attacks which include a grey hole and black hole attack, etc. and structure also contains intrusion prevention devices technique, which gets an input signal from an algorithm and provides the reliable data communication in the network. An intrusion detection system is capable enough of observing the network workload and traffic of these attacks. Besides, fuzzy technique able to investigate and prevent those types of attacks by using well-organized blocking method.

CONCLUSION

In this scholarly article, we have provided fundamental nature of the self-organized mobile ad-hoc network and proficient way of using IDSs that sits on each node of a MANET. Many IDS have been introduced to identify the possible attacks in the MANET. MANETs are unbelievably susceptible to attack due to their dynamically changing topology, the nonexistence of general security, an open medium of communication. MANAT is facing many problems related to the protection. In this survey, reviewed various techniques to secure network and reduce overload and decrease the false alarm rate and energy efficient use of intrusion detection techniques.

REFERENCES

1. R. Chaki, N. Chaki; "IDSX: A Cluster-Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.

2. H. Yang, J. Shu, X. Meng, S. Lu, ”SCAN: self-organised network-layer security in mobile ad hoc networks,” IEEE J. on Sel. Areas in Communications, vol. 24, pp. 261-273, 2006.
3. Jegadeesan,R., Sankar Ram , and J.Abirmi “Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy“ International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018.

4. Yinan Li, ZhihongQian “Mobile agents-based intrusion detection system for mobile ad hoc networks” 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering

5. V. Dinesh Kumar, Dr S. Radhakrishnan Intrusion Detection in MANET using Self Organizing Map(SOM) 2014, International Conference on Recent Trends in Information Technology, IEEE
6. Jegadeesan,R.,Sankar Ram,N. “Energy Consumption Power Aware Data Delivery in Wireless Network”, Circuits and Systems, Scientific Research Publisher,2016

6. AikateriniMitrokotsa, Christos Dimitrakakis “Intrusion detection in MANET using classification algorithms: The effects of cost and model selection”, Journal of Elsevier, 2012

7. Rajesh M, Usha G. Springer Sciences: A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET. Wireless Personal Communications. 2016 September; 90 (2):831-45.
8. Jegadeesan,R., Sankar Ram,N. “Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling”, Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016

9. Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G “Fuzzy-Based Intrusion Detection Systems in MANET” 2nd International Symposium on Big Data and Cloud Computing (ISBCC’15) Procedia Computer Science 50 (2015) 109 – 114

10. Faizal, M.A., MohdZaki M., Shahrin Sahib, Robiah, Y., SitiRahayu, S., and AsrulHadi, Y. “Time-Based Intrusion Detection on Fast Attack for Network Intrusion Detection System”, Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

11. Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference

12. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

13. Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

14. ViswaBharathy, AM, Basha, AM 2016, 'A Hybrid Network Intrusion Detection Technique using Variable Multiplicative K-Means with Self-Organising PSO', Middle East Journal of Scientific research, vol. 24, no. 12, pp. 3812-3819.

15. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

16. ViswaBharathy, AM, Basha, AM, 2016, 'A Detailed Review on Intrusion Detection Systems in Mobile Ad-Hoc Networks Based on Attack Classification and its Detection Technique' in International Journal of Innovative Research in Science and Technology, Vol. 2, no. 9, pp. 228-231.

17. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013)
"Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293.

18. ViswaBharathy, AM, Basha, AM 2017, 'A Multi-Class Classification MCLP Model with Particle Swarm Optimization for Network Intrusion Detection', Sadhana: Academy Proceedings in Engineering Science, vol. 42, no. 5, pp. 631-640.

19. ViswaBharathy, AM, Basha, AM 2016, 'A Hybrid Intrusion Detection System Cascading Support Vector Machine and Fuzzy Logic', World Applied Sciences Journal, vol. 35, no. 1, pp. 104-109.

20. Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1