**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 4, April 2014, pg.660 – 663*

**SURVEY ARTICLE**

# Survey on Network Based Intrusion Detection System in MANET

**Nithya Karthika M[1], Raj Kumar[2]**

[1]P.G Scholar, Department of Computer Science and Engineering, Info Institute of Engineering, Anna University, Chennai, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science and Engineering, Info Institute of Engineering, Anna University, Chennai, Tamil Nadu, India

[1] karthi9187@gmail.com; [2] mail2rajkumar@gmail.com

***Abstract—Mobile Ad hoc Network is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. It is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Network-based intrusion detection systems operate differently from host-based IDSes. The design philosophy of network-based IDS is to scan network packets at the router or host-level, auditing packet information, and logging any suspicious packets into a special log file with extended information. We survey on the intrusion detection system in MANET using various methods and algorithms.***

***Keywords — digital signature algorithm (DSA); Enhanced Adaptive Acknowledgment (EAACK); MANET; IDS***

## I. INTRODUCTION

Network topology changes rapidly and unpredictably over time due to the mobility of the nodes. There arises the need of incorporating the routing functionality into nodes. MANETs are vulnerable to malicious entities that aim to tamper and analyse data and traffic analysis by communication eavesdropping or attacking routing protocols. The identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected.

An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyse data integrity, and more. Depending on the detection methods you choose to deploy, there are several direct and incidental benefits to using an IDS. Understanding what an IDS is, and the functions it provides, is key in determining what type is appropriate to include in a computer security policy.

 

Network-based IDSes have become popular as the Internet grows in size and traffic. IDSes that can scan the voluminous amounts of network activity and successfully tag suspect transmissions are well-received within the security industry. Due to the inherent insecurity of the TCP/IP protocols, it has become imperative to develop scanners, sniffers, and other network auditing and detection tools to prevent security breaches due to such malicious network activity as: IP Spoofing, denial-of-service attacks, arp cache poisoning, DNS name corruption, and man-in-the-middle attacks.

## II. LITERATURE REVIEW

R. H. Akbani, S. Patel, and D. C. Jinwala, [2] 2012, Proposed as, survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Black hole attack and Gray hole attack which are serious threats for MANETs. and also discussed some solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

N. Kang, E. Shakshuki, and T. Sheltami, [7] 2010, Proposed as, There has been a tremendous growth in the use of wireless communication in the past few decades. MANET, Its unique infrastructure less network and self-configuring capability makes it ideal for many mission critical applications, including military use and remote exploration. However, these characteristics also make MANET vulnerable to passive and active attacks due to its open medium, changing topology and lack of centralized monitoring. To address the new security challenges, Intrusion Detection System (IDS) is required to detect the malicious attackers before they can accomplish any significant damages to the network. Many existing IDSs for MANETs are based upon Watchdog mechanism. In this paper, they propose a new IDS called Enhanced Adaptive ACKnowledgement (EAACK) that solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report.

K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, [9] 2007, Proposed as, the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. they analysed and simulation the results to evaluate the performance of the proposed scheme as mention above. A. Singh, M. Maheshwari, and N. Kumar, [15] 2011, Proposed as, an efficient security and trust management based algorithm for MANET. The proposed algorithm consists of three steps: initialization, data transmission, and detection. The time based nonce is generated at different time interval which gives effectiveness to the proposed approach in the sense that it is not easy to detect the generated nonce. The proposed approach is quite effective with the earlier approaches to detect the security threat in MANET.

B. Sun, [16] 2004, Proposed as, Intrusion detection has, over the last few years, assumed paramount importance within the broad realm of network security, more so in the case of wireless ad hoc networks. Intrusion detection systems (IDSs) do just that: monitor audit data, look for intrusions to the system, and initiate a proper response (e.g., email the systems administrator, start an automatic retaliation). As such, there is a need to complement traditional security mechanisms with efficient intrusion detection and response. In this article they present a survey on the work that has been done in the area of intrusion detection in mobile ad hoc networks.

N. Nasser and Y. Chen, [11] 2007, Proposed as, Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols, such as Watchdog/Pathrater and Routeguard. These solutions include two parts: intrusion detection (Watchdog) and response (Pathrater and Routeguard). Watchdog resides in each node and is based on overhearing. Through overhearing, each node can detect the malicious action of its neighbors and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. So they proposed overcome the weakness of Watchdog and introduce our intrusion detection system called ExWatchdog. The main feature of the system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Results shows that their system decrease the overhead greatly, though it does not increase the throughput obviously.

J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, [12] 2004, Proposed as, network intrusion detection (ID) mechanisms that rely upon packet snooping to detect aberrant behavior in mobile ad hoc networks. their extensions, which are applicable to several mobile, ad hoc routing protocols, offer two response mechanisms, passive - to singularly determine if a node is intrusive and act to protect itself from attacks, or active - to collaboratively determine if a node, is intrusive and act to protect all of the nodes of an ad hoc cluster. They implemented their extensions using the GloMoSim simulator and detail their efficacy under a variety of operational conditions.

 

A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, [14] 2005, they present a proof-of-concept implementation of a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent Intrusion Detection System (IDS) for ad hoc networks. Security features in the routing protocol include mechanisms for non-repudiation and authentication, without relying on the availability of a Certificate Authority (CA) or a Key Distribution Center (KDC). And also present the design and implementation details of their system, the practical considerations involved, how these mechanisms can be used to detect and thwart malicious attacks. they discuss several scenarios where the secure routing and intrusion detection mechanisms isolate and deny network resources to nodes deemed malicious.

A. Patcha and A. Mishra, [13] 2003, Proposed as, About The Black hole attack is an important problem that conld happen easily in ad hoc networks especially in popular on demand protocols Like the Adhoc On-demand Distance Vector Rooting (AODV). Prior research in ad hoc networking has generally looked into the routing problem in a nowadversarial network setting, assnming a reasonably trusted environment in This paper they Collaborative architecture to detect and exclude malicious nodes that act in groups or alone. The focus is on the network layer, using the A&hoc On-demand Distance Vector Rooting (AODV) protocol as an example. This paper describes an extension to the watchdog method to incorporate a collaborative architectare to tackle collusion amongst nodes.

K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, [1] 2009, they present an industrial development of a wireless sensor network technology called OCARI: optimization of communication for ad hoc reliable industrial networks. It targets applications in harsh environments such as power plants and warships. OCARI is a wireless-communication technology that supports mesh topology and power-aware ad hoc routing protocol aimed at maximizing the network lifetime. It is based on IEEE 802.15.4 physical layer. An OCARI application layer (APL) is based on ZigBee application support sublayer and APL primitives and profiles to provide maximum compatibility with ZigBee applications. To fully assess this technology, extensive tests are done in industrial facilities at ElectricitEacute De France R&D as well as at Direction des Constructions Navales Services. Their objective is then to promote this specification as an open standard of industrial wireless technology.

T. Anantvalee and J. Wu, [3] 2008, Proposed as, In recent years, the use of mobile ad hoc networks has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. In general, the intrusion detection techniques for traditional wireless networks are not well suited for MANETs. So they classify the architectures for intrusion detection systems (IDS) that have been introduced for MANETs. Current IDS 's corresponding to those architectures are also reviewed and compared. they then provide some directions for future research.

Y. Hu, D. Johnson, and A. Perrig, [4] 2003, Proposed, The design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, they use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol.

Y. Hu, A. Perrig, and D. Johnson, [5] 2002, Proposed as, the attacks against routing in ad hoc networks, and they design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

G. Jayakumar and G. Gopinath, [6] 2007, Proposed as, Recently the introduction of new technologies such as Bluetooth, IEEE 802.11 and hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent revolutions have been generating a renewed and growing interest in the research and development of MANET. To facilitate communication within the network a routing protocol is used to discover routes between nodes. The goal of the routing protocol is to have an efficient route establishment between a pair of nodes, so that messages can be delivered in a timely manner. Bandwidth and power constraints are the important factors to be considered in current wireless network because multi-hop ad-hoc wireless relies on each node in the network to act as a router and packet forwarder. This dependency places bandwidth, power computation demands on mobile host to be taken into account while choosing the protocol. Routing protocols used in wired network cannot be used for mobile ad-hoc networks because of node mobility. This paper reviews and discusses routing protocol belonging to each category in MANET.

S. Marti, T. J. Giuli, K. Lai, and M. Baker, [10] 2000, Proposed as, two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing

 

nodes based upon their dynamically measured behavior. They use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation they evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

## III. CONCLUSIONS

In our survey, Packet-dropping attack has always been a major threat to the security in MANETs. So we need, An intrusion detection system (IDS) where an active process or device that analyzes system and network activity for unauthorized entry and/or malicious activity. The way that an IDS detects anomalies can vary widely; however, the ultimate aim of any IDS is to catch perpetrators in the act before they do real damage to resources. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. Depending on the detection methods you choose to deploy, there are several direct and incidental benefits to using an IDS. In our proposed technique we used Enhanced Adaptive Acknowledgment for intrusion-detection system specially designed for MANETs. And we going to use Digital Signature Algorithm for obtaining a Authentication of message. Regular system checks would verify the proper function of a unit and therefore to reduce the number of malfunctioning units.

## REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Oct. 2009.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana,India, 2012.

[3] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[4] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in P+roc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002.

[5] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom,Atlanta, GA, 2002.

[6] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci.,2007.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc.2010.

[8] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 2011.

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile May 2007.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Mobile Comput. Netw., Boston, MA, 2000.

[11] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE 2007.

[12] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE 2004.

[13] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless 2003.

[14] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc.2005.

[15] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011.

[16] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

 