ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A comprehensive Intrusion detection & discovery technique designed to perform in wireless and Mobile AD-HOC Networks.

G.Vijay Kumar
M.Tech Student(Software Engineering),
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

Jayanthi Rao Madina
Head of the Department,
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

Abstract:

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes.

This results in a highly dynamic, autonomous topology.MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller. The open medium allows MANETvulnerable to attacks. In wired or wireless networks there are many security issues regarding the malicious users in the communication channel. It is very hard to find the malicious users. There are many traditional methodologies to find intruders based on many features such as host system, identity and the way of connecting in network. We introduced a simple identification technique based on the identity of the users by including simple data mining technique to segregation of the users. In our work we designed a novel architecture which contains the abstract version of the network topology.

Keywords:

Wirelss Networks, AD-HoCNetwrorks, Digital Signature,Enhanced Adaptive ACKnowledgment(EAACK). Nodes.

Introduction:

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment.

While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. In computing, a wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization.

Some advanced wireless infrastructure has integrated WIPS capabilities.A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.

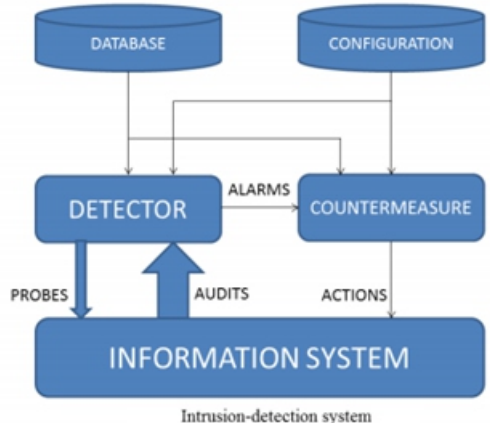
The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Intrusions in a network may happen in various ways:

- Attempted break-in: An attempt to have an unau thorized access to the network.
- Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.
- Penetration: The acquisition of unauthorized access to the network.
- Leakage: An undesirable information flow from the network.
- DoS: Blockage of the network resources (i.e., communication bandwidth) to the other users.
- Malicious use: Deliberately harming the network resources

Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses.

The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.



Intrusion-detection system

The following types of threats can be prevented by a good Intrusion detection and prevention system:

- Rogue AP – WIPS should understand the difference between Rogue AP and External (neighbor's) AP
- Mis-configured AP
- Client Mis-association
- Unauthorized association
- Man in the Middle Attack
- Ad hoc Networks
- MAC-Spoofing
- Honeypot / Evil Twin Attack
- Denial of Service (DoS) Attack

The movement to wireless network from wired network has been a worldwide development in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most significant and distinctive applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; each single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes inMANET-made it popular among critical mission applications like military use or emergency recovery.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

RELATED WORK/BACKGROUND:

1.EAACK-A Secure Intrusion Detection System forMANETS, ElhadiM.Shakshuki, Nan Kang, TarekR.Sheltami, explains various IDS in MANET and itsdisadvantages, EAACK its support in solving falsemisbheaviour report problem.

2. A Survey on Intrusion Detection in Mobile Ad-hoc-Networks in wireless/mobile security, T.AnantvaleeJ. Wu, provides survey of various Intrusion Detectionimplementation in mobile ad-hoc networks.

3.Ad-hoc mobile wireless networks routing protocol-Areview, G.JayakumarG.Gopinath, explains differentrouting protocols like reactive and proactive protocolsand its importance in MANET.

4.Detecting misbehaving nodes in MANETS, N.KangM. ShakshukiT.Sheltami, clarifies the methods inidentifying malicious nodes caused by attacks, and some ways to prevent the network from intruders.

5.Detecting Forged acknowledgments in MANETS, N.Kang E.Shakshuki, specifies the security is based onacknowledgement packets, how to safeguard thosepackets from attacks.

6.Enhanced intrusion detection system for discovering-malicious nodes in mobile ad-hoc network, N.NasserY. Chen, provides an improved technique EnhancedAdaptive Acknowledgement for detecting maliciousnodes in network.

7.A method of obtaining digital signatures and public-keycryptosystems, R.RivestA.ShamirL. Adleman,significant ways of enveloping packets with digitalsignature and public-key cryptosystems.

8.Industrial wireless sensor networks: challenges, principles
and technical approach, V.C.GungorG.Hanke, providesthe various applications of wireless networks inindustries.

EXISTING SYSTEM:

There are three types of intrusion detection methods. They are ID based, Host based and signature based intrusion detection methods. In many of the traditional approaches the intrusion detection based on the user system which consists of the IP Address and the unique port number. Based on the previous connections which are held using IP Address and Port number the classification and the prediction will be done to find the intruder in the network.

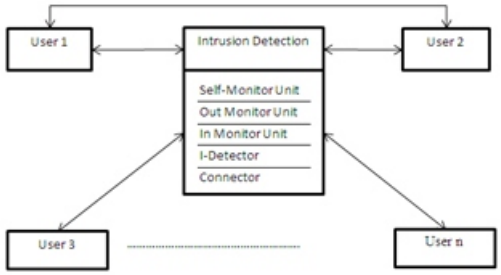
In some of the existing methods users always monitors their incoming connections using firewalls and other security software. In that also there are some limitations such as it blocks all incoming connections including authorized. User always checks the users when is in network communication. There is no possibility to store previous detected symptoms of the intruders. This needs artificial intelligence or machine learning.

After many researches authors included machine learning and artificial intelligence but it needs more storage to maintain the details of users which is connected with each other. So considering all these limitations we introduced a simple and efficient intrusion detection system which is based on the identities of the users.

Proposed System:

In our work we propose a novel architecture of intrusion detection system which consists of a monitor system which initializes in the network when the users connect with each other. Based on the previous connections it classifies the data of the previous connections. It uses artificial intelligence and the architecture below:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



In our architecture there is a special unit which consists of five units with different tasks. Every node contains this unit for security purpose.

Step 1: if any user wants to communicate with another user, he initially sends nodes information to Intrusion Detection Unit. The Detection unit segregates tasks to sub units.Initially the Self monitor unit verifies the source node details and the previous connections of the source node.

Step 2: Out monitor collects information of previous transactions and transfers of the source node. And it collects information about neighbor nodes.

Step 3: In monitor unit maintains the incoming connections to the source node.

Step 4: I-Detector is the main unit of this architecture. It is classifies and predicts the destination is malicious user or not. For we used id based classification method. The classification algorithm is shown below:

This is the supervised learning algorithms based on applying and the assumption of independence between every pair of features. Given a class variable and a dependent feature vector through , states the following relationship:

$$P(y \mid x_1, \ldots, x_n) = \frac{P(y)P(x_1, \ldots x_n \mid y)}{P(x_1, \ldots, x_n)}$$

Using the independence assumption that

$$P(x_i|y, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = P(x_i|y),$$

For all$i$, this relationship is simplified to

$$P(y \mid x_1, \ldots, x_n) = \frac{P(y) \prod_{i=1}^{n} P(x_i \mid y)}{P(x_1, \ldots, x_n)}$$

Since $P(x_1, \ldots, x_n)$ is constant given the input, we can use the following classification rule:

$$P(y \mid x_1, \ldots, x_n) \propto P(y) \prod_{i=1}^{n} P(x_i \mid y)$$

$$\Downarrow$$

$$\hat{y} = \arg\max_y P(y) \prod_{i=1}^{n} P(x_i \mid y),$$

And we can use Maximum a Posteriori (MAP) estimation to estimate $P(y)$ and $P(x_i \mid y)$; the former is then the relative frequency of class y in the training set.
The different classifiers differ mainly by the assumptions they make regarding the distribution of $P(x_i \mid y)$.

In spite of their apparently over-simplified assumptions, classifiers have worked quite well in many real-world situations, famously document classification and spam filtering. They require a small amount of training data to estimate the necessary parameters. The learners and classifiers can be extremely fast compared to more sophisticated methods. The decoupling of the class conditional feature distributions means that each distribution can be independently estimated as a one dimensional distribution. This in turn helps to alleviate problems stemming from the curse of dimensionality.

Conclusion:

In introduced a novel architecture to find the anomalies in the network by introducing the mining of the details of the users in the network. It is reduces maximum attacks in the network. We are performing the connected user classification before exchanging the information in the network. By using various units for various jobs it works more efficiently and reduces more attacks.

REFERENCES:

[1] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar,ATIONS SURVEYS & TUTORIALS, VOL. 16, NO.1, FIRST QUARTER 2014,"A Survey of Intrusion Detection Systems in Wireless Sensor Networks"

[2].R. Rivest, A. Shamir, L. Adleman, A method for obtaining digitalsignatures and public key cryptosystems, Commun.ACM, vol.21,No.2,pp. 120-126, Feb 1983.

[3]. William Stallings, Cryptography and Network Security, Fourth Edition,June 3, 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[4]. G. Jayakumar, G.Gopinath, Ad hoc mobile wireless networks routingprotocol-A review, vol. 3, No. 8, pp. 574-582, 2007.

[5]. T.Anantvalee and J.Wu, A Survey on Intrusion Detection in MobileAdhoc Networks, NewYork: Springer 2008.

[6]. Minimized Routing Protocol in Ad-hoc Network with QualityMaintenance Based on Genetic Algorithm: A Survey, Upasna, Jyoti chauhan, Manisha, IJSRP, vol. 3, Issue 1, January 2013.

[7]. R.H.Akbani, S.Patel and D.C.Jinwala, DOS attacks in mobile adhocnetworks, A Survey in proc. 2nd Int. Meeting ACCT, Rohtak, Haryana,India, 2012,pp.535-541.

[8]. A Secure data transmission in MANETS using Hybrid Scheme, SowmyaThomas, SyamGopi, IJERT,Vol. 2, Issue 8,August 2013.

[9]. Dr.E. Ramaraj, S. karthikeyan, M.Hemalatha, A Design of SecurityProtocol Using Hybrid Encryption Technique(AES-Rijndael and RSA)International Journal of the Computer, the Internet and Management,Vol.17, No.1,(January-April 2009)pp 78-86.

[10]. Y.Hu.D.Johnson, and A.Perrig, and D.Johnson, ARIADNE: A Secureon-demand routing protocol for ad -hoc networks, pp. 3-13.

[11]. Hybrid cryptography by the implementation of RSA and AES,Palaniswamy. V, Jeneba Mary, International Journal of CurrentResearch, Vol. 33, Issue 4, pp. 241-244,april 2011.

[12]. N.Kang, E.Shakshuki and T.Sheltami, Detecting forgedacknowledgements in MANETS, in Proc. IEEE 25th Int. Conf. AINA,Biopolis, Singapore, March 2011, pp.488-494.

[13]. N.Kang, E.Shakshuki, and Sheltami, Detecting misbehaving nodes inMANETS, in Proc. 12th Int. Conf. II-WAS, Nov.2010, pp.216-222.

[14]. K. Liu, J. Deng, P. K.Varshney, and K.Balakrishnan, Anacknowledgment-based approach for the detection of routingmisbehaviour in MA NETS, IEEE Trans. Mobile Computing, vol.6,no.5, pp. 536-550.

[15]. N.Nasser and Y.Chen, Enhanced Intrusion Detection systems fordiscovering malicious nodes in mobile ad hoc networks, in Proc. IEEEInt. Conf. Commun, Glasgow, Scotland, June 2007, pp.1154-1159.

BIOGRAPHIES:

Gandi Vijay Kumar
student in M.Tech(Software Engineering) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.tech in Sarada Institute of Science Technology and Management, Srikakulam. His interesting areas are Data Mining, Networking.

Madina Jayanthi Rao
working as a HOD of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He is pursuing Ph.d at KRISHNA UNIVERSITY Machilipatnam in computer science. He received his M.Tech (CSE) from Aditya Institute of Technology And Management (AITAM), Tekkali. Andhra Pradesh. His interest research areas are Data mining, Image Processing, Computer Networks, Distributed Systems. He published 12 international journals and he was attended number of conferences and workshops.