ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2023; 9(8): 243-249
www.allresearchjournal.com
Received: 05-05-2023
Accepted: 09-06-2023

Prem Prakash Goyal
Research Scholar, Department of Computer Science and Application, Monad University, Hapur, Uttar Pradesh, India

Dr. Deepak Sharma
Research Supervisor, Department of Computer Science and Application, Monad University, Hapur, Uttar Pradesh, India

Corresponding Author:
Prem Prakash Goyal
Research Scholar, Department of Computer Science and Application, Monad University, Hapur, Uttar Pradesh, India

Comparative evaluation of open-source intrusion detection systems: Assessing performance and security in securing computer networks

Prem Prakash Goyal and Dr. Deepak Sharma

Abstract

Research was conducted for this study through a review of existing literature pertaining to intrusion detection systems and how they function. The literature also highlighted previous studies conducted on intrusion detection systems, both commercial and open source. In addition to the review of existing literature, the author conducted independent testing on three open-source intrusion detection systems. The open-source programs, Snort, OSSEC, and Prelude, were selected due to being highly rated in professional publications. The author created a secure simulated computer network, to ensure that each of the programs was tested in a controlled and equitable manner. The findings of this study determined that the three open-source intrusion detection systems tested are as capable as commercial programs in securing a computer network.

Keywords: Computer network, internet protocol, IP address, security, intrusion, open source

Introduction

Till today the researchers have done the research on objective type of question's, today measure problem found in the market is hacking, hanging the network and disturbing the network so with help of Analysis of IP Networks in reference Security Aspects & Performance remove the problem.

1. **Internet Security:** Protocol Version 6 although the primary function of Internet Protocol is to move information through networks, IPv6 holds more promise than IPv4 at its core. Key opportunity Address space is greatly increased. For example, every piece of equipment can have a public IP address so that it can be uniquely tracked. Inventory management of various assets in large distributed organizations such as DRDO. During the inventory cycle, someone must manually verify the location of each personal computer. With IPv6 one can use the network to verify that such equipment is there; even non-IT equipment in the field can also be tracked by having an IP address permanently assigned. IPv6 also has expanded automatic configuration (auto-configuration) mechanisms and reduces the IT burden by making configuration essentially plug-and-play (auto configuration implies that a Dynamic Host Configuration Protocol (DHCP) server is not needed or does not have to be configured).
2. **IPv6 Performance and Gigabit Networks Basic concepts in IPv6 and their security ramifications:** IPv6 (RFC 2460) is a connectionless datagram protocol used to route packets between hosts. However, it has a number of auxiliary features that support the underlying protocol and improve overall performance. Security Aspects of Ad hoc Networks Operating in open and mutual media, wireless communication is inherently less secure than wired communication. In addition, since wireless devices usually have limited properties, such as bandwidth, storage space, processing capability and energy-enforcement of protection is difficult. In comparison with fixed-framework wireless networks, security man agreement for wireless ad hoc networks is more challenging due to unreliable interaction, intermittent connections, node mobility, and constantly changing topology. A complete protection solution should include three components of prevention, detection and reaction and provide security properties of authentication, intimately, non-repudiation, integrity and availability. It should also be flexible enough to properly balance service performance and security performance with resource limitations.

3. **Network Performance:** QoS is the performance level of the services a network provides to its users. The main goal of QoS is to achieve more deterministic behavior through appropriate use of network equipment. A network or service provider can provide different types of services to users based on a set of service requirements, such as minimum bandwidth, maximum delay, maximum delay spread, and maximum packet loss rate. After accepting the user's service request, the network must ensure that the user's service requirements are met through the entire communication. QoS provisioning is rebellious due to key characteristics of MANET such as lack of centralized federation, host mobility and limited resource availability.

Security of Mobile Adhoc Networks (MANET), operating in an open and shared environment, wireless communication is more insecure than traditional communication. Additionally, security is difficult to use, as mobile wireless devices often have limited resources such as bandwidth, storage, processing power, and energy. Compared to fixed wireless networks, security management in wireless ad hoc networks is more difficult due to unreliable communication, network inconsistency, mobility and changing topology. A security solution should include the three aspects of prevention, detection and response and provide security features of authentication, confidentiality, non-repudiation, integrity and availability.

It also needs to be flexible enough to balance service performance and security with limited usage.

Mobile Network Security Fundamentals

There are two types of wireless networks: wireless local area networks (WLANs) and wireless/mobile ad hoc networks. The first must use one or more access points (or base stations). These access points connect wireless users and manage their access to the Internet and other WLANs. The ad hoc communication format is based on radio-to-radio multi-hop.

As wireless devices are on the move, wireless/mobile ad hoc networks, or MANETs for short, have evolved to serve an increasing number of tasks, including military communications, emergency rescue operations, and rescue efforts. Taking advantage of the ease of deployment, wireless ad hoc networks are very effective. Compared to a wireless local area network, the wireless ad hoc network has tighter security control and generally has the following features:

1. **Restricted usage:** Wireless networks often have bandwidth limitations, memory, and processing power. This means that expensive solutions won't work on wireless ad hoc networks.
2. **Unstable communication:** The shared state and unstable channel quality of the wireless link can cause packet loss and unstable redirection, a common phenomenon that causes damage to multihop network. This means that security solutions in wireless ad hoc networks cannot rely on effective communication.
3. **Node Mobility and Dynamic Topology:** The network topology of wireless adhoc networks will change rapidly and unpredictably over time as connectivity between nodes may change over time due to node exit, node arrival, and node mobility range.
4. **Scalability:** Due to the limited memory and processing power of mobile devices, scalability is an important issue when we consider large networks. Networks of 10,000 or even 100,000 nodes are seen, and scalability is a major concern. Performance in the wireless ad hoc network is close to energy security. However, security is worthless without good network performance. Therefore, in this section, we will cover network performance issues in the development of security systems, not cryptanalysis or security code analysis.

Real-time communication security should consider the following

Authentication

Authentication is the process of verifying the identity of the sender of the communication. Without authentication, attackers can easily access resources, obtain sensitive information, and interfere with other nodes' operations.

Privacy

Privacy means that only authorized recipients can access some information.

Parties dealing with emergencies must cooperate with each other while maintaining the confidentiality of traffic across the network.

Non-rejection

Non repudiation ensures that the originator of the message cannot deny that the message was sent. It is useful in the diagnosis and isolation of diseases.

Integrity

Integrity is the property that messages cannot be edited without being examined. Without integrity, it is easy for attackers to corrupt and modify data, causing mobile devices to make incorrect decisions based on incorrect data.

Availability

Availability Ensures the survival of network services under denial-of service attacks. In unreliable wireless communication with highly dynamic topologies, there can be an impact on network performance.

Dedicated communications is an emerging field in mobile computing. The wireless nature of communication and the lack of security infrastructure cause many security-related issues. Important questions about these areas are addressed here.

Need for Research in Ad hoc Networks: In a large Network, an infected node is difficult to track down. Attacks from nodes are more dangerous and harder to detect.

Therefore, every part of the wireless ad-hoc network must be able to operate in a peer-trusting mode. The Ad-hoc network has a distributed function and many Adhoc network algorithms rely on the cooperation of node members. Enemies can exploit the lack of centralized decision making to develop new attacks by disrupting their engagement algorithms. Also, ad-hoc forwarding is simpler than expected because most ad-hoc communication methods are collaborative in nature. An attacker intercepting ad hoc nodes can completely destroy the entire network by spreading illegal information that could cause all nodes to provide information for the nodes to tamper Intrusion prevention technologies such as encryption and authentication can reduce the risk of intrusion, but cannot completely eliminate the risk of intrusion, meaning encryption and authentication cannot prevent interactions between nodes.

Overview of Intrusion Detection Techniques: In general, an "attack" is defined as "any action that attempts to compromise integrity, confidentiality, or resources".

Systems and processes designed to provide services can be the target of attacks such as Distributed Denial of Service (DDOS). Intrusion detection can be used as a second line of defense to protect network connections because when an intrusion is detected, action can be taken to mitigate harm or gather evidence for prosecution or opposition.

Intrusion Detection assumes "users and processes are visible"; this means that all user-or application-initiated processes have accessed a system table or location in some system type that Intrusion Detection Systems (IDS) can easily access for these system logs. This data/data recorded about users is called audit data. That is, penetration investigation is about the capture of audit data and based on the audit data it is determined whether there is bad behavior and if so, the IDS determines that the system has been hacked. Depending on the type of data analysis, IDS can be divided into 2 types

a) **Network-based:** The network based IDS resides at the gateway and captures and analyses network packets passing through the network hardware interface.

b) **Host-based:**

The Host based IDS relies on data analytics processes to monitor and analyze events generated by the host's users or services.

In the case of wireless networks, only audit data is limited to radio communications, and an IDS designed for such networks should use quasi and local data control. IDS's standard anomaly detection cannot be used in wireless ad-hoc networks as the dividing line between normal and abnormal is blurred. Nodes sending incorrect data (production) may be corrupted or currently out of sync due to physical failure. Therefore, in wireless ad hoc networks, it is difficult to distinguish false positives from true intrusions. IDS the new (paid) architecture of IDS must be deployed and coordinated to meet the needs of wireless ad hoc networks.

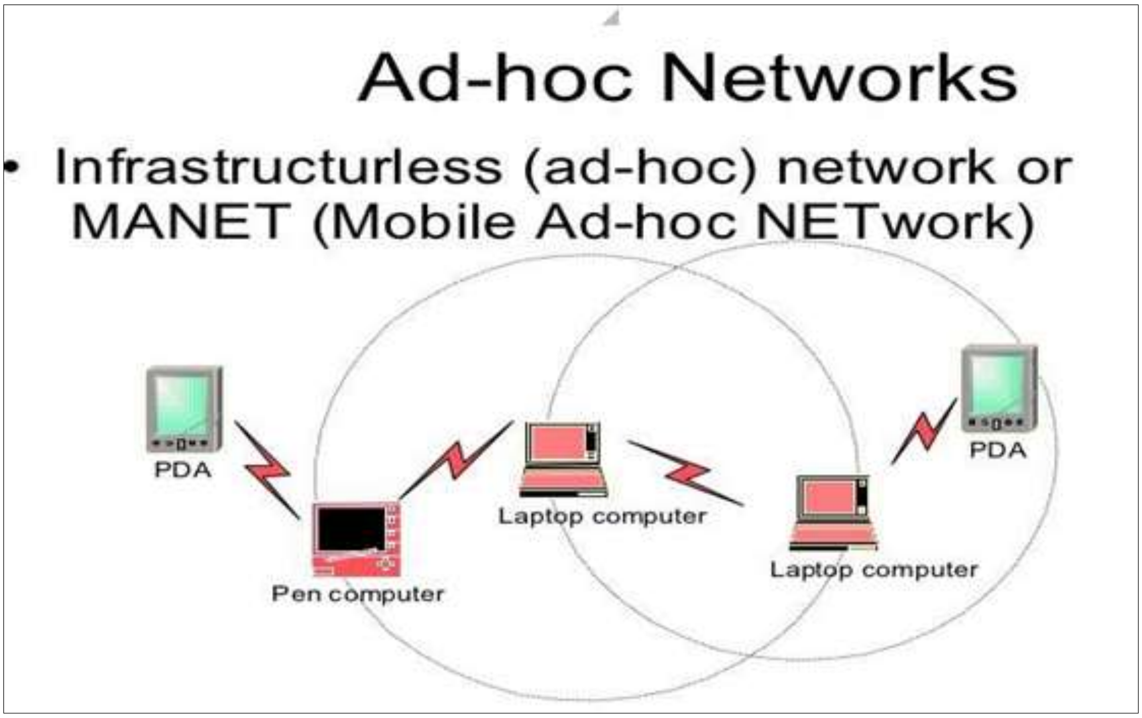
Ad-hoc Networks
• Infrastructurless (ad-hoc) network or MANET (Mobile Ad-hoc NETwork)
PDA
Pen computer
Laptop computer
Laptop computer
PDA

Fig 1: The IDS Architecture for Mobile Ad-hoc network

An IDS agent falls within the following criteria, i.e.,

1) **Local Data Collection:** Local Data Collection module collects real-time audit data from various sources that can be seen on user and mobile activity, communication between node and radio communication between node and this Node.
2) **Local Detection Engine:** The local detection engine checks local inspection data for evidence of suspicious activity. This requires IDS to apply certain rules for the nodes that the audit log will examine. But as more devices go wireless, the types of attacks planned against these devices will increase, making current experts' policies inadequate for this new attack.

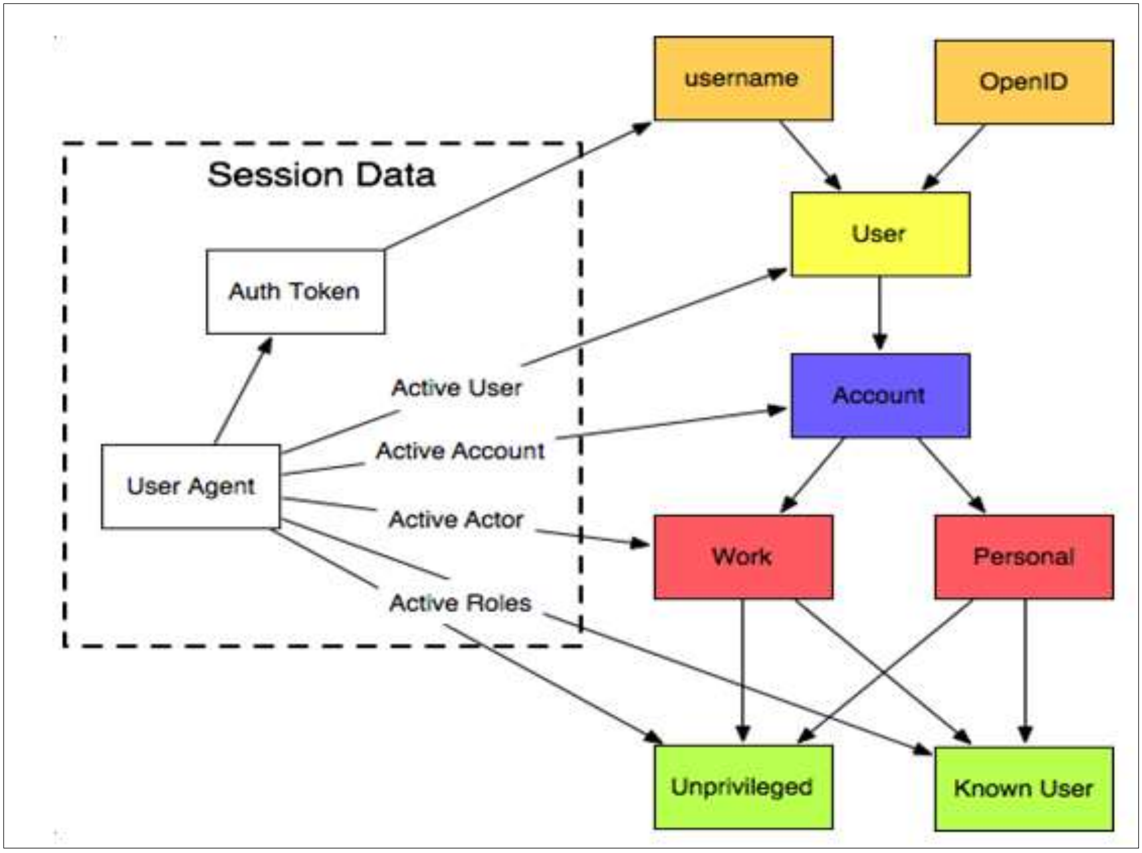

Fig 2: Conceptual model for an IDS agent

3) **Collaboration detection:** If a node finds a local attack with strong evidence, it can independently decide that the network is under attack and begin as a response or treatment. However, if the evidence of suspicious or intrusion is weak or suspicious, the node decides that it needs further investigation and can initiate the global access process, which will include sending access information to search the status of neighbors and continue to the Network. If necessary

1. A node sends an "access status request" to its neighbours.
2. Each node, including the node that started the algorithm, then spreads the state information indicating the potential entry to its immediate neighbours.
3. Each of them determines whether most of the information received indicates intrusion, and if so, concludes that the network is under attack.
4. Any node that sees the network access can initiate the repair/response process.

As a general rule, information controlled by other nodes should not be trusted, as interceptors can send false information.

However, there is no incentive for interfering nodes to send audit data, and doing so could create a situation where nodes are removed from the network. Therefore, the repair process will not start unless most of the nodes are affected and at least one is valid.

Detection of Abnormal Updates in Routing Tables Legal changes in meetings are due to physical movement of nodes or changes in network attendance. For a node, its movement and the change of its meeting is the only information it can rely on, so we use it as the basis for tracking information. Physical movement is measured by distance, direction, and speed. Routing table change is measured by path percent percent (PCR) and total count count (PCH). We use percentage because the number of nodes/paths is not fixed due to the weak nature of wireless ad hoc networks.

During the "training" process, various normal situations are simulated and correlation data are collected for each. Audit/system information for all nodes in the network is then combined to obtain the process of all changes in the meeting of all nodes. The profile always shows the relationship between the physical movements of the nodes and the changes in the routing table. Algorithm classification of data is available in many forms. Now for specific tracking information, if the PCR and/or PCR value is outside the valid range (velocity, direction and distance) for the specific movement, it is considered abnormal and the necessary action is started.

Detection of faults in other layers Trace information for MAC protocol, all channel requests in the last S seconds, requests by all nodes, etc. may form. This class can satisfy the current request of the node. A classifier that monitors the data defines the profile of a request. An abnormal detection pattern can be calculated based on the deviation of the data line from the normal profile.

Likewise, at the wireless application layer, the service can be used as a class and have the following properties all requests to the same service in the last S seconds, total cases, average service time, number of requests. Service is waiting for all service errors.

A service worker always defines the behavior and demand of each class of service.

Key Management in Wireless Networks From a security standpoint, several lines of defense must be used to prevent attacks. A complete wireless self-driving network security solution should have three parts: protection, detection and response.

Solving security

a) Symmetric key management Symmetric key systems such as DES, AES, and cryptographic hash functions rely on key information of communication between two parties. In this case, if the sender uses a key to encrypt the message, the receiver will use the same key to decrypt the message. Symmetric key technology is attractive because of its power efficiency. Therefore, many technologies have been developed for a certain type of communication (wireless sensor networks), since electronics is cheap and low power.
b) Symmetric-key cryptography, the sender and receiver must make a mutual agreement before they can communicate. In the context of sensor networks, shared secrets are distributed to sensors before transmission. With limited memory resources, it is very difficult to create a useful deployment plan in large networks with the following two problems:

Connections: A percentage of neighboring sensor nodes must share at least one key.

Resistance: When some nodes are affected by the enemy, other sensors can still maintain secure communication. (b) Random key distribution. Has three phases of key distribution:

1) Key pre-distribution.
2) Shared key discovery.
3) 444-path (1)) create values. During pre-delivery.

Limited resources: Mobile nodes are often powered by batteries of different capacities. There are many people like MANET. Identification algorithms should be considered with limited resources. For example, Exploit based detection algorithms should include memory signatures and malicious detection methods should be optimized to minimize resource usage.

Collaborative: MANET routing protocols are generally collaborative. This makes them targets for new attacks. For example, a node may act as a neighbor to other nodes and participate in the decision making process that will affect the importance of the network.

Recommended Intrusion Detection System (IDS) MANET's IDS uses a variety of intrusion detection methods. By far, the most frequently reported method of finding access is specification-based search. This can detect attacks on communication at low cost. Some exploits have been developed for MANETs, such as IDS and little research has been done on signature attacks against MANETs. Modifying signature attacks is a critical issue for this approach.

Some systems use monitoring of wireless communication around nodes. Because the nodes in the MANET only have local information, an integrated IDS architecture is often used to provide a more comprehensive detection method. In this model, each node has its own local IDS representative and communicates with representatives of othernodes to exchange information, make decisions, and respond. Other IDS architectures in MANET are single hierarchical IDS [1].

In a single IDS architecture, every part of the network has an IDS agent and independently detects attacks without cooperating with other nodes. Such models are usually not important, as they cannot use some of the network data at the root of the source to detect network attacks (network scanning, distributed attacks, etc.).

Hierarchical IDS is also an integrated system. In this model, the network is divided into clusters, regions, etc., where some nodes (cluster heads, interregion nodes, etc.) play a larger role than other nodes in the same group (communication with other groups, region).

Each head of the group/region conducts the regional investigation, and the group head and time conduct the global investigation. It is suitable for multi-layer networks [1].

It is believed to provide high detection at low cost. SVM Light was found to outperform RIPPER. It has also been shown that processes that have a relationship between changes in different data types (position, orientation, etc.) perform better, so reactive processes (on-demand) are better than table driven protocol for this process. Additionally, IDS is said to work better with processes that contain some redundancy, such as redundancy in DSR. However, the consequences of liquid processing are indisputable. This can reduce the negative effects from the movement of nodes. However, it only shows local activity and not network connectivity. Also, every device must have a built-in GPS (Global Positioning System) to receive this moving information. From a security perspective, the system will be reliable as long as most of the nodes are not compromised. (These may send false information. Nodes in a region are called region nodes, and nodes that act as bridges are called range (gateway) nodes.

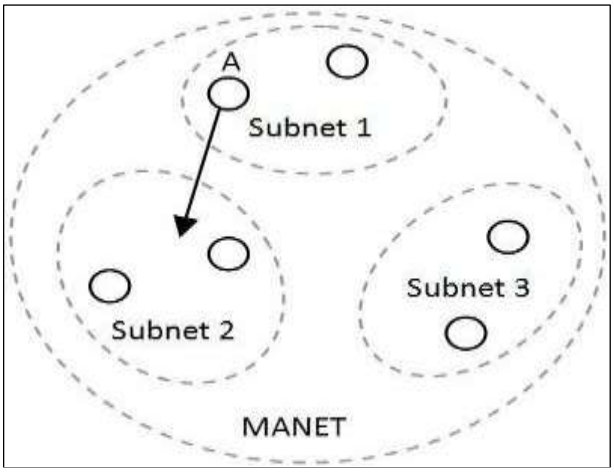

Fig 3: Zone-based IDS architecture in MANETs

As shown in Figure 3, there can be multiple gateways in an area, for example nodes 1, 6, 7 are gateway nodes in area 5. Each node in the area is responsible for local investigations and reporting to the area. Interregional nodes. Frames are designed to allow different detection methods to be used on each IDS agent; however, they only used Markov chain anomaly detection in their study. The input for the IDS agent is the update table (PCR and PCR) in.

Nodes in the domain do local aggregation and issuance and gateway nodes are responsible for global aggregation and arranging, making the final decision and sending the alarm. Therefore, only gateway nodes are involved in access discovery. Reports sent by cross-region nodes only show an estimate of access probability; (c) A Generic Collaborative Intrusion Detection Architecture. A collaborative and efficient hierarchical IDS architecture using multiple layers is proposed. Figure 2 shows a network with two level clusters. Nodes marked "1" are basically the first level management group, acting as the management focal point for IDS activities of immediate neighbors. Firstlevel group leaders can form groups around the senior "2" and the second group.

This process continues until all nodes are assigned to the cluster. Select more than one header for the parent group to avoid any malfunction. The criteria for defining the head include topology, proximity, anti-interference, power efficiency and bandwidth. Anomalous Node Detection Nodes in MANET rely on other nodes to send their packets.

However, these intermediate nodes may behave differently by dropping or exchanging these packets. Here are a few tips on how to identify such behavior.

a) Watchdog & Pittwater

This is the basis for detecting bad behavior (nodes not performing their assigned tasks) and mitigating its effects. Since ad hoc networks rely on the cooperation of all nodes for routing and forwarding to increase overall network throughput, as discussed in [15], misbehaving nodes will be critical to network performance. In this paper, a tracking and pathrater mechanism of DSR is aimed to improve the throughput of the network in the presence of misbehaving nodes.

Nodes can be abusive because they can be excessive, selfish (seeking to protect their own resources), malicious or ineffective.

Watchdog and Patrater with/without SRR was evaluated on four different levels of NS simulator using utility, overhead, and defect ratio as metrics. Results showed that Watchdog and Pathrater increased delivery by 17% in the presence of moderate motion with 40% negative muscle tone and 917% overhead. According to the movement, they increase by up to 27% and increase the overall load from 12-24%.

b) Discrimination

This is a method presented in [4] for detecting and responding to negative behaviors that stem from the biological concept of mutual altruism. It detects faulty nodes and responds by not sending their packets. The aim of this approach is to improve integrity, robustness and coordination in MANETs.

Each part of the mission is to monitor the behavior of their next neighbors and look for bad behavior. Each node has a trust architecture and FSM, and each node has four main components: Monitor, Domain Name, Route Manager and Trust Manager. The Reputation system (node ratings) maintains local listings and/or blacklists that can be exchanged with friends.

One of the tests can be modified when there is sufficient evidence and according to the frequency of bad behavior [15]. The cost function also uses weights as a source of poor detection. Self-knowledge has the highest weight, observation has a lower weight, while information reported from other nodes has a weight to the reliability of the nodes. Reputation systems only use negative experiences; Research on quality change and timing still needs attention. The Node trust level is instead managed by the deployed Trust Manager.

It is also responsible for sending notifications and filtering messages sent by other nodes. The trusted node plays an important role in exchanging routing information with the node, using it for routing or forwarding and accepting routing requests.

Route manager can respond to requests from different routes, such as ignore request, respond to node, respond to all requests with bad behavior by sending a warning to the center of the site and redefine the route. And remove the path, including negative behavior [4].

c) Lightweight Packet Loss Detection (LiPaD)

Anjum and Talpade [2] provides a method for detecting packet loss attacks. In this way, each part counts the packets it receives and sends and periodically reports this count to the partner.

Each node is responsible for monitoring its packets in LiPaD. The algorithm performed by each of these is very simple, useful for limited resources. On the other hand, usage of network bandwidth can be important because each node sends a report from the destination and destination IP to the coordinator of each stream. Instead of sending each stream in a single packet, they recommend compressing and aggregating data from multiple streams. However, it can still affect network connectivity, especially in networks with hundreds of nodes. Agent node (analyzing reports from all nodes) will have heavy computation. The organization node must be a powerful tool and at the same time secure, because it can be the target of an attack that affects the search mechanism.

For example, it could be the target of a DoS attack (via the broadcast medium). Since the coordinator node observes the same data flow from all nodes in the path, it is possible to catch false nodes with information about their own data individually to the coordinator node [2]. If all nodes in the path are cooperative and malicious, LiPaD cannot detect packet loss attacks in that path.

d) Response to Intrusion Detection

Open Issues and Future Scope

MANET is a new technology that is increasingly used in many applications. These networks are more vulnerable than the telephone network. Due to their different characteristics, security measures cannot be applied directly. Researchers are now focused on developing new protection, detection and response systems for MANETs. IDS guide for different MANETs, Mobility, node capacity and network infrastructure are important features that are often studied for MANET IDS planning. For very large networks, IDS using poor detection methods will experience poor results. In addition to mobility, the capacity of the node must also be taken into account. For nodes with limited resources, a simple discovery process may be appropriate.

For example, the method in uses a reduced set without a reduced detection rate. Obviously, the network infrastructure plays an important role in choosing an IDS.

It can also modify the IDS according to its own rules and characteristics. For example, it can change the structure of the IDS option or combine different intrusion detection techniques. Therefore, defining the rules and specifying the characteristics of the network is very important in determining the best IDS solution.

Conclusion

This paper focuses on addressing structures and protocols.

Benefits

1. Reduce the problem of IP networks with this study.
2. Use this investigation to find the cause of the problem.
3. Increase the efficiency of the network without data and destroy data.
4. Expand IP network addressability.
5. A more efficient and reliable mobility mechanism.
6. Scalability of IP networks.

The present paper presents a brief overview on network analysis as a statistical approach for health psychology researchers. Networks comprise graphical representations of the relationships (edges) between variables (nodes). Network analysis provides the capacity to estimate complex patterns of relationships and the network structure can be analysed to reveal core features of the network. This paper provides an overview of networks, how they can be visualised and analysed and presents a simple example of how to conduct network analysis in using data on the Theory.

Control systems are expensive and not guaranteed to be secure. Various protocols have been proposed to work in ad hoc networks. To meet the needs of these networks, they need to be more secure and robust. Intrusion detection is an essential part of the security response.

But in a bad Adhoc environment this is an invisible target. However, the simplicity, ease and speed with which these networks can be created means they will find wider use. This leaves adhoc networks open to research that will satisfy demanding applications. Intrusion detection of these complex systems is a growing and immature area of research. Compared to traditional networks, fewer IDSs are recommended for MANETs Researchers can focus on introducing new IDSs or modify existing systems to address specific MANET tasks. Hybrid approaches can also be effective. The applicability of the architecture to the environment is important in an IDS design. False positives can be greatly affected by the level of movement. A system must be aware of its traffic and existing network topology.

Therefore, information about the movement should be included in the access to find out if the working system has been created. As nodes are the only source of information in the network, all nodes must contribute to the IDS by providing local monitoring, discovery and local information to other nodes as needed. However, nodes may have different computational capabilities, some of which are not sufficient to perform complex or large access search algorithms. The limited resources issue is currently being investigated. Researchers may decide to design different algorithms for different nodes depending on their resources and/or computing power.

In this paper, we explore IDS research on MANETs. Many MANET IDS have been proposed with different methods of access detection, design and response methods. We focus on everyone's contributions/innovations and identify specific MANET issues that not everyone is talking about. The proposed method mainly deals with some MANET problems. MANET has most of the problems of wired networks and more.

Therefore, MANET's access detection is still a difficult and challenging task for security researchers.

References

1. Jain R. Congestion control in Computer Networks: Issues and Trends, IEEE Network Magazine. 1990 May-Jun;4:24-30.
2. Mogul JC. IP Network Performance, in Internet System Handbook, Lynch, D.C and Rose MT. (eds.); c1993. p. 575-675.
3. Anantvalee T, Wu J. A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Chapter 7, Springer. Edited by Xiao Y, Shen Y, Du DZ; c2006. p. 170-196.
4. Anjum F, Talpade R. LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks, Proceedings of IEEE Vehicular Technology Conference (VTC). 2004;2:1233-1237.
5. Axelsson S. Intrusion Detection Systems: A Survey and Taxonomy, Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology; c2000.
6. Buchegger S, Le Boudec J. Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Network, Proceedings of 10th Euromicro Workshop on Parallel, Distributed and Network-based Process; c2000. p. 403-410.
7. Guha R, Kachirskio, *et al.*, Case-Based Agents for Packet-Level Intrusion Detection in Ad-Hoc Networks, Proceedings of 17th International Symposium on Computing & Information Science; c2002. p. 215-230.
8. Heady R, Luger G, Maccabe A, Servilla M. The architecture of a network level intrusion detection systems, Technical Report, Computer Science Department, University of New Mexico; c1998.
9. Huang Y, Fan W, *et al.*, Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies, Proceedings of 23rd IEEE International Conference on Distributed Computing Systems (ICDCS). 2003;23:478-487.
10. Huang Y, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks, Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; c2003. p. 135-147.
11. Huang Y, Lee W. Attack Analysis and Detection for Ad Hoc Routing Protocols, Proceedings of Recent Advances in Intrusion Detection; c2004. p. 125-145. LNCS-3224.
12. Abdrabou A, Zhuang W. A position-based QoS routing scheme for UWB mobile ad hoc networks. IEEE J Select. Areas Commun. 2006;24:850-856.
13. Ahn GS, Campbell AT, Lee SB, Zhang X. Insignia. Internet Draft; c1999. comet.columbia.edujinsigniajdraft-ietf-manet-insignia-01.txt Accessed 18 March 2008.
14. Ahn GS, Campbell AT, Veres A, Sun LH. Supporting service differentiation for real-time and best effort traffic in stateless Wireless Ad Hoc Networks (SWAN), IEEE Transactions on Mobile Computing. 2002;1(3):192-207.
15. Badis H, Agha KA. QOLSR: QoS routing for ad hoc wireless networks using OLSR. Wiley European Transactions on Telecommunications. 2005;15(4):427-442.
16. Barolli L, Koyama A, Shiratori N. A QoS routing method for ad-hoc networks based on genetic algorithm. Proc. 14th Int. Wksp. Database and Expert Systems Applications; c2003. p. 175-179.
17. Bharghavan V, Demers A, Shenker S, Zhang L. MACAW: A media access protocol for wireless LANs. Proc. ACM SIGCOMM, 1994, 212-225.