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
IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 3, March 2020, pg.10 – 18

Deep Analysis of Intrusion Detection System for Mobile Devices with Networking System

Sonu Devi[1]; Dr. Anuj Kumar Sharma[2]
[1]M. Tech Scholar, Department of Computer Science & Engineering
[2]Associate Professor, Department of Computer Science & Engineering
[1, 2]Om Institute of Technology & Management, Hisar

Abstract: An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. MANETs have various defining characteristics that differentiate them from other wired and wireless networks. MANETs are formed based on the collaboration between independent, peer-to-peer nodes that wish to communicate with each other for a particular purpose. No prior organization or base station is defined and all devices have the same role in the network. In addition, there are no pre-set roles such as routers or gateways for the nodes participating in the network unless specific arrangements are provided. Wireless links that connect the MANET nodes have much smaller bandwidth than those with wires, while the effects of interference, noise and congestion are more visible, causing the available bandwidth to vary with the surrounding conditions and to be even more reduced. MANET depends on radio frequency (RF) or infrared (IR) technology for connectivity, both of which are generally short range. Therefore, the nodes that wish to communicate directly need to be in close proximity to each other. To overcome this limitation, multi-hop routing techniques are used through intermediate nodes that act as routers to connect distant nodes.

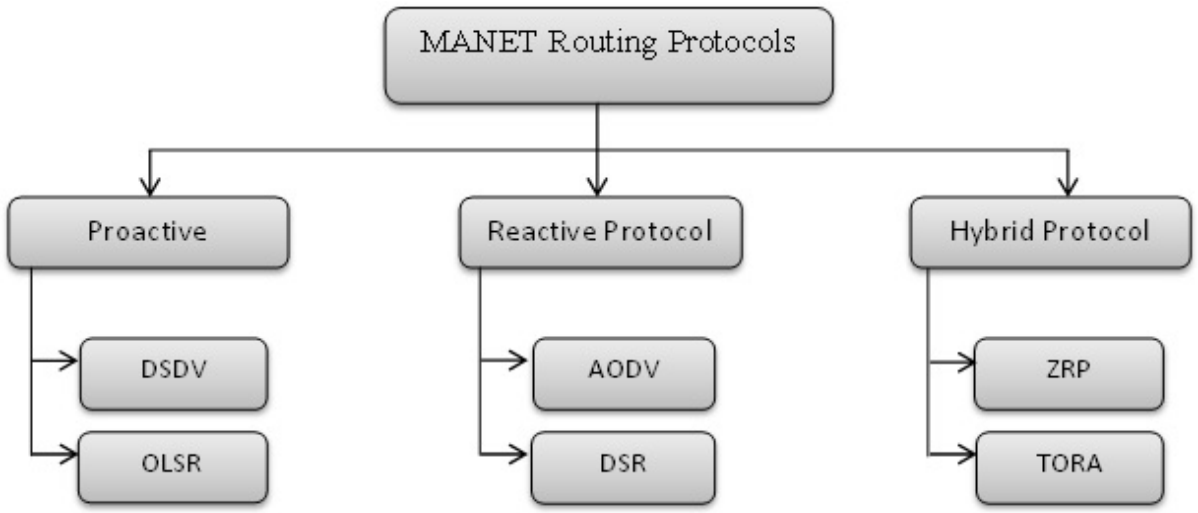
Keywords: MANET, Radio frequency, Intrusion Detection System, Information Technology

Introduction

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behaviour is observed,

the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.



Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

Detection Method of IDS:

Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis

of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

Anomaly-based Method:

Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Gray Hole Attack

Gray hole Attack is a similar to black hole attack except it uses selected shortest paths for route paths can drop the selected forwarding hopes only. It can be easily launched over AODV routing protocol because it highly depends on the hope count and sequence numbers. Whenever sender transmits a route request, it is intercepted by intruder nodes and they alter the route request with their own and send its fake reply with minimum delay. After receiving the route reply, legitimate nodes just update their routing tables and introduce the intruders in the network. After all, elder node stats transmission of data which is selectively dropped by the intruder nodes and only few packets are further forwarded.

Network simulator (NS)

Network simulator (NS) was introduced by UC Berkely. It uses two different languages i.e. C++ and Tool Command Language (TCL). It supports various application, protocols and traffic types to simulate the wired and wireless networks.

Protocols under investigation are: Authenticated Routing for Ad Hoc network guards against active attacks i.e. fabrication and modification but network resources are compromised due to heavy computation of asymmetric cryptographic methods. Security aware ad hoc routing is able to find out secure optimal path without fulfilling security requirements. Trusted AODV provides the secure routes on the cost of extra control overhead thus may lead to low efficiency. ARIADNE provides end to end point security but could not encounter intruder

nodes. Secure efficient ad hoc distance vector can protect the network from DoS attack but does not guard against worm hole attack. Secure routing protocol deals with spoofing using Hash functions and can also observe the routing data in dept. but cannot recognize the modified cache and network may be compromised by worm hole attack.

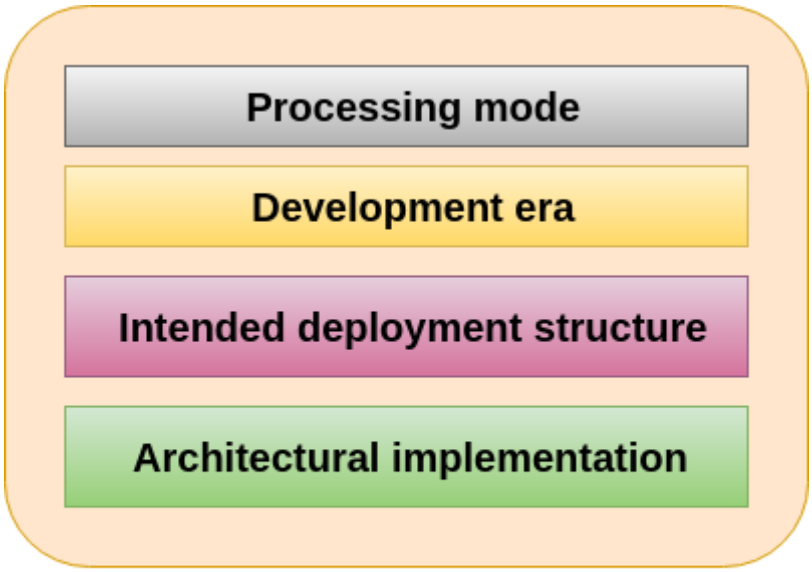
Simulation results show that in case of Blackhole attack, variations in performance parameters are inversely proportional to the density of intruders. As the number of intruders increase, packet delivery ratio and Throughput both are decreased while delay is increased. On other hand, Gary hole attack has less impact over the same performance parameters.

Firewall

Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.

Categories of Firewalls

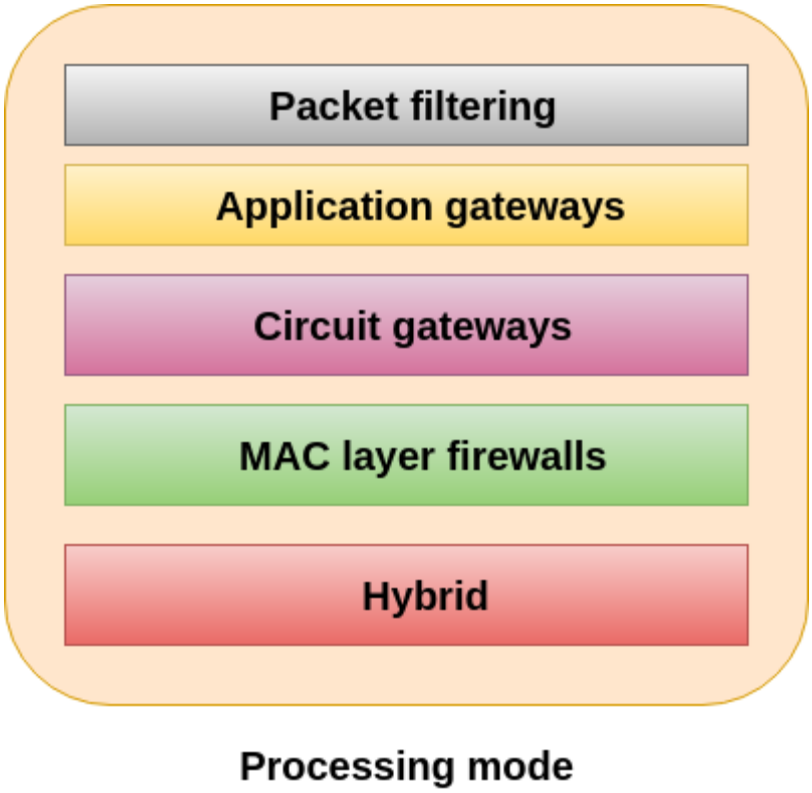
Firewall can be categorized into the following types-



Categories of Firewalls

1. Processing mode:

The five processing modes that firewalls can be categorized are-



Processing mode

Packet filtering

Packet filtering firewalls examine header information of a data packets that come into a network. This firewall installed on TCP/IP network and determine whether to forward it to the next network connection or drop a packet based on the rules programmed in the firewall. It scans network data packets looking for a violation of the rules of the firewalls database. Most firewall often based on a combination of:

Internet Protocol (IP) source and destination address.

Direction (inbound or outbound).

Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests

Packet filtering firewalls can be categorized into three types-

Static filtering: The system administrator set a rule for the firewall. These filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed.

Dynamic filtering: It allows the firewall to set some rules for itself, such as dropping packets from an address that is sending many bad packets

Stateful inspection: A stateful firewalls keep track of each network connection between internal and external systems using a state table.

Application gateways

It is a firewall proxy which frequently installed on a dedicated computer to provides network security. This proxy firewall acts as an intermediary between the requester and the protected device. This firewall proxy filters incoming node traffic to certain specifications that mean only transmitted network application data is filtered. Such network applications include FTP, Telnet, Real Time Streaming Protocol (RTSP), BitTorrent, etc.

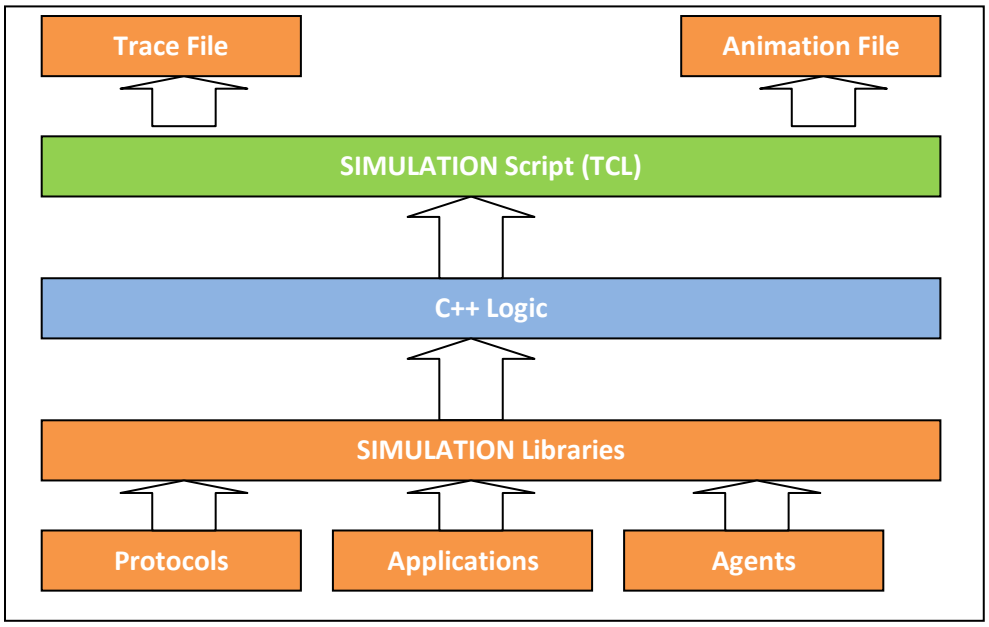
Circuit gateways

A circuit-level gateway is a firewall that operates at the transport layer. It provides UDP and TCP connection security which means it can reassemble, examine or block all the packets in a TCP or UDP connection. It works between a transport layer and an application layers such as the session layer. Unlike application gateways, it monitors TCP data packet handshaking and session fulfillment of firewall rules and policies. It can also act as a Virtual Private Network (VPN) over the Internet by doing encryption from firewall to firewall.

MAC layer firewalls

This firewall is designed to operate at the media access control layer of the OSI network model. It is able to consider a specific host computer's identity in its filtering decisions. MAC addresses of specific host computers are linked to the access control list (ACL) entries. This entry identifies specific types of packets that can be sent to each host and all other traffic is blocked. It will also check the MAC address of a requester to determine whether the device being used are able to make the connection is authorized to access the data or not.

Network simulator (NS) was introduced by UC Berkely. It uses two different languages i.e. C++ and Tool Command Language (TCL). It supports various application, protocols and traffic types to simulate the wired and wireless networks.



Conclusion

NIDS can be also combined with other technologies to increase detection and prediction rates. Artificial Neural Network based IDS are capable of analyzing huge volumes of data, in a smart way, due to the self-organizing structure that allows INS IDS to more efficiently recognize intrusion patterns. Neural networks assist IDS in predicting attacks by learning from mistakes; INN IDS help develop an early warning system, based on two layers. The first layer accepts single values, while the second layer takes the first's layers output as input; the cycle repeats and allows the system to automatically recognize new unforeseen patterns in the network. This system can average 99.9% detection and classification rate, based on research results of 24 network attacks, divided in four categories: DOS, Probe, Remote-to-Local, and user-to-root.

This research work is related to detection and prevention of Grayhole attack over MANET using AODV routing protocol. As per the literature survey, it can be observed that various researchers have already developed the different solutions to secure the MANET but each have its own strength and limitations. A self-organized Grayhole detection scheme was proposed in this research work. Proposed scheme analysis the routing information as well as the node behavior. Attack detection at node level has a advantage over the existing scheme

i.e. traffic analysis can be performed at node level and if there is any change in routing information, entire network is informed. Analysis is performed using sequence number, route discovery, packet forwarding and packet drop. If a packet is forwarded but it is intentionally dropped, then threshold value is updated and each node is aware from this information. If frequent changes occur in sequence number that is also monitored because AODV uses these sequence numbers to keep the information about fresh routes but in case of gray hole attack, selected routes are observed and highest fake sequence number is introduced and replaced with the fresh one and after capturing the route information, finally forward data is dropped at that route.

Now we discuss the simulation results of proposed scheme under the constraints of various parameters i.e. Throughput, Packet delivery Ratio and Routing Load. In normal network environment, Throughput is 54 bps, but during attack phase, if one intruder node is active then, It reduces upto 34bps, in case of 2 active intruders, it further decreased upto 29.9 bps and finally it is reduced upto 0.4 bps due to the four intruder nodes which have the highest impact over the network performance.

Proposed scheme can detect and recover from attack and maintains Throughput upto 34.9 bps, with two intruder nodes, It can maintain Throughput upto 34.2 bps and in case of four intruders, it can recover Throughput upto 23.5 bps.

In case of normal network environment, PDR is 66.9975186%, in compromised network, it varies w.r.t. intruder node's density. In case of single intruder node, it reduces upto 42.1836228%, with two intruders, it is 37.0967742 and four intruders reduce it upto 0.49627792%.

Proposed scheme recovers from attack and in the presence of single intruder, it is 43.3002481%, with two intruders, it is 42.4317618% and with four intruders, it is 29.1563275%.

Routing load variations under different simulation scenarios. It is 2.49259259, in normal network environment but increased upto 202.5, in case of compromised network. Using proposed scheme, it is reduced upto to 4.42978723.

References

[1]. McAfee Labs, 2018. Threats Predictions 2018, description available at: http://mcaffee.com

[2]. Indian Express (2019) "Cyber bullying new-age threat" Indian Express.

[3]. Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others by Bruce S. Schaeffer, Henfree Chan, Henry Chan and Susan Ogulnick.

[4]. MIT Geospatial Data Centre, 2019. Cyber security and human psychology.

[5]. McAfee Labs, 2019. Threats Predictions 2014,description available at: http://mcaffee.com

[6]. Didwania, P (2019) "India: Cyber Defamation In Corporate World" available on http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+Word

[7]. Cyber Crime 2015 https://www.emc.com/collateral/white-paper/rsawhite-paper-cybercrime-trends-2015.pdf

[8]. Research on Improved ECC Algorithm in Network and Information Security.

[9]. An Improved Weighted Clustering for Ad-hoc Network Security New by Basant Kumar Verma and Binod Kumar, 2019.

[10]. Network Security with Cryptography by Prof. Mukund R. Joshi, Renuka Avinash Karkade, 2019.

