HIDS

Host Intrusion Detection Systems are run on individual hosts and devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the administrator of suspicious activity is detected. [9]

Anomaly Detection

In anomaly Detection both user and system behavior can be predicted using normal behavior patterns. Anomaly detectors identify possible attack attempts by constructing profiles representing normal usage and then comparing it with current behavior data to find out a likely mismatch. For specified, well-known intrusion excellent detection results are achieved by signature-based methods. But, they cannot find out unfamiliar intrusions though constructed as a least alteration of previously known attacks. Conversely, the capability of discovering intrusion events which are previously unobserved is the main advantage of anomaly based detection techniques.

Fuzzy logic

Fuzzy rules are key tools for expressing pieces of knowledge in "fuzzy logic". However, there neither exist a unique kind of fuzzy rules, nor is there only one type of "fuzzy logic". Main task of fuzzy rules is to provide accurate decision within some specific environment.[12][13] . Fuzzy logic is an innovative technology which enhances conventional system design with engineering expertise. The use of fuzzy logic can help to circumvent the need for mathematical modeling. Fuzzy logic is a extended version of conventional logic, and fuzzy logic controllers are a extension of linear extended version of control models. Hence anything that can be built using conventional design techniques can also be built with fuzzy logic, and vice-versa. However, in a number of cases, conventional design methods would have been complex and, in many cases, might prove simpler, faster and more efficient. The key to successful use of fuzzy logic is its combination with conventional techniques. Also, a fuzzy system is time-invariant and deterministic. Therefore any verification and stability analysis method can be used with fuzzy logic, too.[14]

Network intrusion detection system using fuzzy logic:

In view of the fact that there is no ideal solution to avoid intrusions from event, it is very significant to detect them at the initial moment of happening and take necessary actions for reducing the likely damage. Several researchers focused on fuzzy rule for effective intrusion detection. In this system, anomaly-based intrusion detection makes use of effective rules identified in accordance with the designed strategy. The fuzzy rules generated from the proposed strategy can be able to provide better rate in detecting the intrusion behavior. This proposed system consists of fuzzy logic-based system for effectively identifying the intrusion activities within a network. The proposed fuzzy logic-based system can be able to detect an intrusion behavior of the networks since the rule base contains a better set of rules.

2. Literature Review

Details of different existing methods for intrusion detection:

- Statistical Model: These techniques try to differentiate between the normal and abnormal behavior based on some parameters that are collected over time. Examples include bandwidth, CPU utilization, user session time, etc. These parameters collected eventually, are used to create profiles for individual users/activities. If the values of these parameters go beyond what has been learnt as normal about the entity, an intrusion is flagged[18].
- Data Mining Based Methods: The strength of IDS is improved by periodically updating the rules and data by an expert system. This process is manual and, therefore, time consuming [17][18].
- Signature analysis: This method behaves like the basic misuse detection technique and looks for the patterns of data in the audit trials. This method is very similar to knowledge based systems but the complexity regarding the semantics of attacks as in expert systems is very low in this technique.[18]
- Genetic Algorithms: This method is simply based on the concept of human genome systems. Through continuous monitoring it evolves and develops a data structure called chromosomes which represent the problems to be solved. These are machine learning based techniques and are called evolutionary algorithms or evolutionary computations. Eventually, rules are generated which judge the intrusions and their counter measures. If a condition for that rules is met, then a set of predefined actions is performed. Since biological parameters are involves, it involves a higher degree of resource [18][16].
- State transition based: This method uses the finite state theory as a basis for detecting intrusions. It denotes various network states as states of a finite state machine. If a sequel state is identified from the network state of finite state machine, an intrusion is detected. The method represents the intermediate steps of a penetration as states that must lead to an intrusion. The graphical representation of intrusions makes it easier to derive the intrusions from the intermediate states that must take place for the successful completion of an intrusion. In addition to these initial and compromised states, there exist some states known as signature states that represent the actions that would prevent an intrusion if they are omitted.[18]
- Expert based systems: In earlier days of development, the data called audits produced by IDS was forwarded to an administrator (a human) who used to analyze those long log files and check for suspicious. The disadvantage of this method was time consuming and exhaustive study of audit trials. Recently computer machines have been developed with human like knowledge and reasoning maintained as a knowledge base. These are in fact used by knowledge based IDS techniques. In addition to this knowledge base there is a set of rules and heuristics that is applied on this knowledge base to trap intrusions, if any.[18]
- Petri nets: They are knowledge based systems that use mathematical models to represent the states of a system graphically. A knowledge based Petri net model, that uses

Colored Petri nets has been developed at PURDUE University. The vertices of the graph represent the system states and the transition from one state to another is marked by events. Three parameters must be satisfied – pre-condition which identifies the actions that must occur before the pattern matching, post actions which define the actions after the pattern matching and invariants which are the conditions looked for during the process of pattern matching.[18]

3. Details of Proposed System

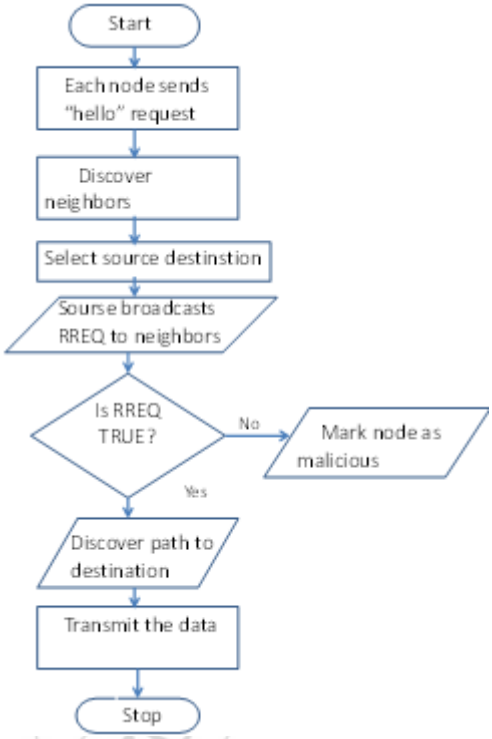
The proposed system will combine anomaly detection algorithm with the decision making based on fuzzy rules. In this method we will extend anomaly detection algorithm with fuzzy rules that what will be the output of anomaly detection algorithm will be given to fuzzy rule base system to take decision about intruders. Up till now fuzzy rules are only used in case of misuse detection technique which has been proved most accurate for misuse detection but for anomaly detection still there is requirement for accurate technique to detect intruders with more accuracy. Anomaly detection algorithm is based on the fact that the probability of a connection attempt being a success should be much higher for a benign host than a malicious one.

3.1 System Overview

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device it is not a stand-alone protection measure. In this simulation module applied IDS module will protect through the malicious behavior if malicious node is in the range of IDS. At first IDS will check which node update the routing table and send higher sequence number to the sender node, if find out so IDS will send the message to the sender node to eliminate that particular path where belongs Malicious node and search new route according to IDS instruction. Here internal module of IDS provides only protection of misbehave and provide trust communication between sender and destination. After prevention we detect malicious node via trace analysis and provide secure communication in wireless network. This will further be continued for finding types of attack in the network and that attacked node will get removed and communication between nodes will get continued.

In this proposed system each node in the network will send "HELLO'' message to all neighboring nodes. that node will either reply to that node or rebroadcast it to its neighbor by increasing hop count. Source node will wait up to certain time limit for getting reply from receiver. If (node replied which is not a neighbor of source) then mark it as malicious. If (Any two nodes send the same next hop) It will forward to the one that has sent the "HELLO" first. Else Source will select the first two nodes that has send the "HELLO" first and send a dummy packet by encrypting it with the public key of corresponding next hop. When the next hop receive the packet it will send 2ACK to the sender by encrypting that acknowledgment by its private key. The sender forwards the ACK to source node. The source node gets ACK from one node or both nodes or may not get any acknowledgement. If (It get ACK from only one node) It will mark the node not malicious by updating from 1 to 0 in Is Malicious entry and send the packet through it and mark the other node malicious. If (It get ACK from both node) It will send the packet though the one having less hop count and update both as non malicious. If (It does not get ACK from any node) It will mark both nodes malicious and will choose next two nodes from the Collection of Route Reply and repeat previous step [4].

3.2 Flowchart of Proposed System



3.3 Types of attacks detected by proposed system

- Blackhole attack

Blackhole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter.

- Selfishnode attack

This malicious node which is also known as selfish node and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is

involved. Therefore these selfish node behaviors are known as selective existence attacks. For instance, selfish nodes do not even send any HELLO messages and drop all packets even if they are sent to it, as long as it does not start the transmission. When a selfish node wants to start a connection with another node, it performs a route discovery and then sends the necessary packets.[19]

- Gray Hole Attack (Routing Misbehavior)

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose th connection to destination then they may want to discover a route again, broadcastin RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior.

4. Experimental results of proposed system:

Figure 2: Dedtected 3 types of attack

Advantage of proposed system: One important limitation to NIDSs is the frequency of false positives. No current IDS can completely eliminate the possibility of a false positive.[15] So this propose system of IDS with fuzzy logic will try to reduce this false positive by extending decision part of IDS with fuzzy logics.[1]

5. Conclusion and Future Scope

5.1 Conclusion

Application of fuzzy rules to IDS for a computer network within a purview of information security methodologies based computing enhances the decision making ability of the IDS and in turn network. Such a system will improve the performance of the network significantly as the frequency of malicious activities of a member in the network will be reduced to a certain extent due to uncovering of such activities a quick action can be taken to prevent such harmful members from affecting the normal behavior of the network.

5.2 Future Scope

- In future, more complex fuzzy rules can be included to capture more complex and dynamic situations arising in the network.
- In this study, the AODV routing protocol is used. But the other routing protocols could also be used. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Attacks may be determined.
- Some more types of attack can be determined

References

[1] Sergei Dotcenko, Andrei Vladyko, Ivan Letenko. *"A Fuzzy Logic-Based Information Security Management for Software-Defined Networks"*2014 IEEE International Conference.
[2] Dotsenko S.M., Vladyko A.G., Letenko I.D. "Intrusion detection systems based on embedded microprocessor systems"Telekommunikatsii (Telecommunications) № S7 (2013): 15-18.
[3] Vladyko A.G., Letenko I.D., Dotsenko S.M. "Network protection system" RU Patent RU 133954 U1 G06F21/00 (2013.01)
[4] Shin, Seugwon, et al. "FRESCO: Modular composable security services for software-defined networks."
[5] Mehdi, Syed Akbar, Junaid Khalid, and Syed Ali Khayam. "Revisiting traffic anomaly detection using software defined networking." Recent Advances in Intrusion Detection.Springer Berlin Heidelberg, 2011
[6] Schechter, Stuart E., Jaeyeon Jung, and Arthur W. Berger. "Fast detection of scanning worm infections."Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2004..
[7] Williamson, Matthew M. "Throttling viruses: Restricting propagation to defeat malicious mobile code." Computer Security Applications Conference, 2002.Proceedings.18th Annual. IEEE, 2002..
[8] Cingolani, Pablo, and Jesus Alcala-Fdez. "jFuzzyLogic: a robust and flexible Fuzzy-Logic inference system language implementation." Fuzzy Systems (FUZZ-IEEE), 2012 IEEE International Conference on.IEEE, 2012.Proceedings of Network and Distributed Security Symposium. 2013.
[9] http://netsecurity.about.com/cs/hackertools/a/aa030504.ht
[10] http://eduscapes.com/tap/topic121.htm
[11] "computer system security" by William stalling.
[12] What are fuzzy rules and how to use them D Dubois, H Prade - Fuzzy sets and systems, 1996
[13] " Induction of fuzzy rules and membership functions from training examples" by Tzung-Pei Hong"**, Chai-Ying Leeb
[14] http://www.electronicsforu.com
[15] NSRP: Intrusion Detection Systems
[16] Susan M. Bridges, Associate Professor Rayford B. Vaughn," Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection" Associate Professor Department of Computer ScienceMississippi State University
[17] Y.Dhanalakshmi 1 and Dr.I. Ramesh Babu 2," Intrusion Detection Using Data Mining Along Fuzzy Logic and

Genetic Algorithms" IJCSNS International Journal of Computer Scienc e and Network Security, VOL.8 No.2, February 2008

[18] Uzair Bashir, Manzoor Chachoo" Intrusio Detection and Prevention System: Challenges Opportunities". 978-93-80540/14/$31.00_c2014IEEE

[19] "Investigation of Blackhole Attack on AODV in MANET" , Anu Bala, Raj Kumari and Jagpreet Singh, © 2010 ACADEMY PUBLISHER doi:10.4304/jetwi.2.2.96-100

[20] "A NOVEL DEFENCE SCHEME AGAINST SELFISH NODE ATTACK IN MANET", Gaurav Soni1 and Kamlesh Chandrawanshi2 DOI:10.5121/ijcsa.2013.3305.