Scholarly Research Journal for Humanity Science & English Lang
Online ISSN 2348-3083, SJ IMPACT FACTOR 2016 = 4.44, www.srjis.com
UGC Approved Sr. No.48612, OCT- NOV 2017, VOL- 4/24

LESSAR METHODOLOGY FOR NETWORK INTRUSION DETECTION

Kazi Kutubuddin Sayyad Liyakat

Abstract

In wireless sensor network there are a few routing algorithms, which use topology information to make routing decisions at every node. Subsequently extensions to existing position based routing algorithm have been portrayed to work all the more productively indeed in situations where they are not working at present. Development of hosts brings about a change in routes, obliging some system for deciding new routes. A few routing protocols have already been proposed for ad hoc networks. The essential thought is to permit the cellular beneficiaries encountering poor channel conditions to utilize the ad hoc network to connect to those cellular collectors that are encountering great cellular channel conditions.The current article describes then implementation of lesser algorithm for analysis of network intrusion detection system in wireless sensor networks.

Keywords: *Wireless, Network, Sensor*

INTRODUCTION: A few improvements to the implementation and simulation model are talked about along with simulation specifics. New situation visualization instruments for portability design generation and examination are portrayed. A bland skeleton and excercise for creating new ad-hoc routing simulation models are additionally introduced. The simulation model created is utilized to look at the execution attributes of OSPF-MCDS to three distinctive institutionalized wireless routing protocols. Simulation outcomes introduced here show that no single protocol can attain ideal execution for all portability cases. Distinctive observations from simulation tests are outlined that backing the feasible competitor for diverse portability situations. The scope of wireless information services is expanding rapidly and changing from largely voice oriented to increasingly data and multimedia services. The trends in future commercial wireless services include increasing data traffic, internet protocol (IP) telephony, and multimedia applications. The integration of computing and wireless communication will facilitate future mobile application. In addition, the growing interest is accessing the wired network anytime anywhere has driven the developments of mobile ad hoc networks which can be used in many Realistic applications.

An example application of ad-hoc network is that a group of soldiers move in outdoors while communicating with one another through the radios. Without a central controller to control

the communications in the network, without a fixed topology, the most difficult task the Ad-Hoc network faces is routing. Much work has been done on routing in ad-hoc networks, but most of them focus only on best-effort data traffic.

The secure communication provisions are derived from wire line networks where the control and signaling rely on a circuit model that requires explicit connection management and the establishment of hard-state in the network prior to communication. However, out-of-band signaling needs to maintain source route Information and respond to topology changes by directly signaling intermediate routers on an old path to allocate/free radio resources. In many case, this is impossible to do if the affected router is out of radio contact from the signaling entity. By the same token, the hard-state approach lacks flexibility to adapt to the dynamics found in mobile ad hoc networks. Based on this analysis we propose a new secure communication architecture that can provide fast reservation, responsive restoration and seamless adaptation to mobile ad hoc network dynamics.

Quality-of-service (Secure Communication) is the qualitatively or quantitatively defined performance agreement between the service provider and user applications based on the connection requirements. The Secure Communication requirements of a connection are a set of constraints such as bandwidth (available bandwidth) constraint, delay constraint, jitter constraint, loss ratio constraint, and so on.

The Secure Communication condition of a network reflects the networks ability to provide the specified service between communication pairs. Because of the rising popularity of multimedia applications and real-time services, which require strict bandwidth/delay constraints, together with the potential commercial usage of Ad-Hoc networks, Secure Communication support in the MANET has become a topic of interest in the wireless area.

Many Secure Communication components should work together to support Secure Communication in Ad-Hoc networks: a Secure Communication model specifies which kinds of services to be included in the network; a Secure Communication routing scheme searches a path with satisfactory resources defined by the Secure Communication model; a Secure Communication MAC protocol solves the problems of medium contention; a Secure Communication signaling protocol performs the resource reservation along the path computed by the Secure Communication routing protocols.

NETWORK INTRUSION DETECTION USING LESSAR ALGORITHM

In the LESSAR algorithm, a global time is maintained in wireless sensor networks by organizing the whole network system into levels. Level discovery is performed initially when the network is deployed. Sink which collects information from all nodes forms the root andisassignedlevel0.Itbroadcastsleveldiscoverypacket to its neighbors. Nodes receiving the packets are assigned level 1 and broadcast the level discovery packet to the other nodes. One node may as a result, receive many packets but it accepts only the one with the lowest level Asitsancest or and take sits value+1as its own level. Thus broadcasting continues. All the sensor nodes are connected in this hierarchical Network topology. When a new node enters, it broadcasts the level request packet to enquire the current level value so fits neighbors. From the responses obtained, its elects the smallest one+1 As its level. On node failure, its children notice this, when its timer of observing keep alive message expires. These nodes broad cast level request packet and redo the level discovery process again.

This algorithm may be extended to provide connected coverage for a set of finite regions.

Step 1: [Initialize]
Let s be any leaf of the Euclidean minimum-cost spanning tree of the point set.
$candidateSet = \{s\}$

Step 2: [Deploy Sensors]

while ($candidateSet \neq \emptyset$) {
Remove any point p from $candidateSet$.
Place a sensor at p.
Remove from $candidateSet$ all points covered by the sensor at p.
Add to $candidateSet$ all points (not necessarily vertices) q
on the spanning tree T that satisfy the conditions:
(1) q is distance r from p.
(2) q is not covered by an already placed sensor.
(3) The spanning tree path from s to q is completely covered by already placed sensors.
}

Algorithm 1: Lesser Algorithm for Point-set

In LESSAR, nodes are synchronized level by level. Each node believes that the clocks in it supper level are accurate than its local clock and synchronize with them. It only accepts time sync packets from the upper level and drops all others from the lower levels. So The whole wireless sensor network follows the clock of the sink. This will be synchronized by GPS/NTP. This method h as very lower source consumption and computation complexity. To deal with the energy management problem, different power management

schemes are discussed here. The most important constraint in all wireless sensor networks is the *Energy efficiency* problem since they are equipped with limited power sources. So an efficient power management should be adopted. Research is conduct educing static approaches to attain power management by making the nodes which are not currently being utilized to go to low power states but this should be decided earlier, in a fixed time schedule and not atrun time.This algorithm overlays

Step 1: [Construct Local Neighborhood Graph]
Each sensor broadcasts its id and location.
Each sensor s compiles a list $L(s)$ of all ids and locations that it hears.
Let $A(s)$, the adjacency list for s, comprise all sensors $a \in L(s)$ such that there is no $b \in L(s)$ located in the interior of the intersection region of the radius $|sa|$ circles centered at s and a.
For each $a \in A(s)$, the weight of the edge (s, a) is $|sa|/2$.

Step 2: [Construct Best Support Path]
Let the length of a path be the maximum weight of its edges.
Let x and y, respectively, be the sensors closest to the points u to v.
Run the distributed Bellman-Ford shortest path algorithm to determine a shortest path $P(x, y)$, in the local neighborhood graph, from x to y.
$(u, x), P(x, y), (y, v)$ is a best support path from u to v.
The weight of (u, x) is $|ux|$ and that of (y, v) is $|yv|$.
$SW(u, v)$ is the maximum of the edges weights in the best support path.

Algorithm 2: Lesser Algorithm for Neighborhood Graph

Dynamic Power Management (DPM) is widely used in wireless sensor networks. During run time, dynamic techniques can further improve there eduction in power consumption by selectively shutting down the hardware components. After designing A system, additional power savings can be obtained by Dynamic Power Management. Protocols and algorithms have to be tuned for a n application . Embedded operating systems and software become acritical requirement of such networks. Major consumer of energy in a wireless sensor network is the energy communication circuits. So communication should be performed only when needed. DPM should always consider when an ode should go to sleep/idle state and how long it shoul drema in there. Sensor nodes communicate using short data packets which have more dominance of start up energy. External events represent the interaction between the sensor node and the environment. So DPM involves shutting down the sensor node during no event and waking Them up when needed. So good energy saving is achieved. But sensors communicate using short data packets. So there is more dominance of startup energy. Therefore DPM should becare fully implemented. Operation in energy saving mode becomes energy efficient only if the times pent in that mode is greater than a decided Threshold. The common DPM policies are the Predictive policy and the Stochastic policy.

Step 1: [Transmit the packets for $S_n, \cdots, S_2$]
Transmit the packets for $S_n, \cdots, S_2$, in this order.
For this transmission, use slots $2j-1$, $1 \leq j \leq t$, where $t = \sum_{l=2}^{n} p_l$.
The base station makes no transmission in slots $2j$, $1 \leq j \leq t$.

Step 2: [Transmit S_1's packets]
The packets destined for S_1 are transmitted in slots $2t < j \leq 2t + p_1$.

Algorithm 3: Lesser Algorithm for Base Station

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or security standard practices. To understand the meaning of intrusion detection, we can use an analogy to the common "burglar alarm". Just like the burglar alarm, intrusion detection works on a computer system or network and is enabled to detect possible violations of security policies and raise an alarm to notify the proper authority.

DISCUSSION

A Network Intrusion detection System (NIDS) is an intrusion detection system that tries to detect malicious activity such as service attacks, port scans or even attempts to break into computers by monitoring network traffic. It is a fact that most firewalls are configured and deployed by humans. And human beings are prone to error making. This knowledge is well-known to the intruders who try to take advantage of it. They try to find a security breach in the configuration of the firewall and exploit it. As most organizations deploying security mechanisms use encryption for protecting files and external network connections, so the intruder's interest will lie on such locations where the encryption/protection of data transmission is missing or very minimal. This is generally the case where the data is stored and/or transmitted to trusted hosts and networks. Even if a VPN request connection is made between trusted hosts and networks and the main network in question, attacks by intruders can be very efficient. Furthermore, the probability of successful attacks in this type of attacks can be very high as, in most cases, not even minimum encryption is used for increasing performance.

Address spoofing is a method which is used to hide the real address of the sender of a network packet, particularly the intruder. However, this can also be used to bypass the firewall and gain unauthorized access to a network or computer. Contemporary firewalls have

in-built mechanisms to avoid this fraud. They are, practically, not deceived by this kind of address spoofing. But the principle of address substitution, in itself, remains an urgent issue that needs to be addressed.

For instance, an intruder can mask her own address with the address of a trusted network address or with the address of a trusted host in the network and send packets containing malicious data which may adversely affect the network computers and data. This method is different from the attack by trusted host and network problem since in this case only the address of the trusted host is used rather than masquerading as the trusted host in the former case.

As the firewall software and hardware are built by humans, they themselves are prone to attack from the intruders. A successful attack on the firewall can lead to very serious consequences as once successfully attacked, intruders can freely access the resources of the protected network without the risk of being detected and traced. Moreover, an intruder can also tweak with the configuration and rules of the firewall to allow other kind of intruders to attack the network.

A network intrusion detection system reads all incoming packets and tries to find suspicious patterns known as signatures or rules. These rules are decided by a network administrator while the configuration and deployment of the network intrusion detection system based on the security and network policies of the organization. For instance, if it is observed that a particular TCP connection requests connection to a large number of ports, then it can be assumed that there is someone who is trying to conduct a port scan of all/most of the computers of the network.

A network intrusion detection system is not limited to inspecting the incoming network traffic only. Patterns and outgoing intrusion can also be found from the outgoing or local traffic as well. Some attacks might also come from the inside of the monitored network, as in trusted host attack.

At the heart of every modern network intrusion detection system there is a string matching algorithm. The network intrusion detection system uses the string matching algorithm to compare the payload of the network packet and/or flow against the pattern entries of the intrusion detection rules, which are a part of every network having a network intrusion detection system.

In many cases, intruders try to and penetrate firewalls to gain unauthorized access to corporate networks. This is done by attacking the firewall itself and breaking it down by tweaking its rules and signatures. In this case, the network intrusion detection system can decrease the risk of such attacks by temporarily backing up firewalls. The network intrusion detection system of this type filters packets based on their IP packet header. This enables the network administrator to deploy network intrusion detection systems with functionality comparable to that of very advanced firewalls. Further, this type of network intrusion detection system can also be used while the general firewall is down for maintenance or when the firewall software is being updated or for any other reason.

SIGNIFICANCE OF THE STUDY

Generally functions of controlling file access are done to specialized systems, such as Secret Net, which are intended specifically for protecting network information from unauthorized access. However, protection of some critically important files such as database files and password files cannot be done by such systems. Moreover, such systems are mainly developed for the Windows and NetWare platforms. So such systems fail in UNIX environments which are used for network applications in many organizations. So in such types of cases a network intrusion detection system comes to the rescue of network administrators. Mainly host based network intrusion detection systems are used in such cases which are based both on log-file analysis (Real Secure Server Sensor) and IDSs analyzing system calls (Cisco IDS Host Server).

A network intrusion detection system can help in identifying the address of unknown/external hosts within the protected network segments. It can also detect increased traffic and special kind of activities from specific workstations which were not involved in such kind of activities before. Such activities can be a hint to malicious activities from the hosts and the network administrator must be informed about this.

Firewalls are essential for protecting the corporate network from unwanted network activities. But a firewall can work desirably only when it is configured correctly. Incorrect configuration and inefficient testing of a firewall can wreak havoc on the network. Installing a network intrusion detection system before and after the firewall allows one to test the efficiency of the firewall by comparing the number of attacks before and after the firewall. In addition to this, it can also act as a backup for the firewall.

CONCLUSION

Log files from routers and other network equipment can serve as an additional source of information on the various attacks that a data network can be prone to. However, most organizations do not analyze this collected information because it is a time overhead for the organization and the tools available for such analyses (such as net Forensics) are rather costly.

A network intrusion detection system can be configured to do this work. The task of collecting such log-file information and analyzing logged security events can be delegated to the intrusion detection system, which in this case, serves as a Syslog server. It can centralize such tasks of collecting log-file information and detect attacks and misuse of the network. It also prevents unauthorized modifications of the events logged. Moreover, the events logged are immediately sent to another server so that the intruder can't remove any traces after completing her operation.

Most network administrators use the default network configurations for simplifying their tasks. But this also simplifies the task of an intruder because she knows the default network configurations. This makes the network more vulnerable and open to successful attacks. A network intrusion detection system can be configured to search the hosts where default configurations have been used and can also recommend corrective measures that can be taken.

REFERENCES

Gungor, V. C., Lu, B., & Hancke, G. P. (2010). Opportunities and challenges of wireless sensor networks in smart grid. Industrial Electronics, IEEE Transactions on, 57(10), 3557-3564.

Ergen, S. C., & Varaiya, P. (2010). TDMA scheduling algorithms for wireless sensor networks. Wireless Networks, 16(4), 985-997.

Akyildiz, I. F., & Vuran, M. C. (2010). Wireless sensor networks (Vol. 4). John Wiley & Sons.

Stabellini, L., & Zander, J. (2010). Energy-efficient detection of intermittent interference in wireless sensor networks. International Journal of Sensor Networks, 8(1), 27-40.

Chiwewe, T. M., & Hancke, G. P. (2012). A distributed topology control technique for low interference and energy efficiency in wireless sensor networks. Industrial Informatics, IEEE Transactions on, 8(1), 11-19.

Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. Computer Networks, 54(15), 2688-2710.

Baccour, N., Koubaa, A., Mottola, L., Zuniga, M. A., Youssef, H., Boano, C. A., & Alves, M. (2012). Radio link quality estimation in wireless sensor networks: a survey. ACM Transactions on Sensor Networks (TOSN), 8(4), 34.

Tang, L., Sun, Y., Gurewitz, O., & Johnson, D. B. (2011, May). EM-MAC: a dynamic multichannel energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing (p. 23). ACM.

Incel, O. D., Ghosh, A., Krishnamachari, B., & Chintalapudi, K. (2012). Fast data collection in tree-based wireless sensor networks. Mobile Computing, IEEE Transactions on, 11(1), 86-99.

Baccour, N., Koubaa, A., Mottola, L., Zuniga, M. A., Youssef, H., Boano, C. A., & Alves, M. (2012). Radio link quality estimation in wireless sensor networks: a survey. ACM Transactions on Sensor Networks (TOSN), 8(4), 34.

Tang, L., Sun, Y., Gurewitz, O., & Johnson, D. B. (2011, May). EM-MAC: a dynamic multichannel energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing (p. 23). ACM.

Incel, O. D., Ghosh, A., Krishnamachari, B., & Chintalapudi, K. (2012). Fast data collection in tree-based wireless sensor networks. Mobile Computing, IEEE Transactions on, 11(1), 86-99.