INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 555-562
RECEIVED : 04/03/2016. PUBLISHED : 15/03/2016

Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes

Varalakshmi.S, Pg Scholar, Dept of CSE, Mahendra Engineering college, Namakkal,
Umamaheswari.A, Asst prof, Dept of CSE, Mahendra Engineering college, Namakkal.

Abstract:

Mobile Ad-Hoc Networks(MANET) geared towards routing efficiency. The resulting protocols tend to various attacks. Number of solutions has been proposed for different types of attacks however these solutions often compromiserouting efficiency or network overload. One major attack is DDOS attack against the OptimizedLink State Routing protocol (OLSR) known as the node isolation attack. It occurs whentopological knowledge of the network is exploited by an attacker who is able to isolate the victimfrom the rest of the network. In this project, it suggests a novel solution to defend the OLSRprotocol from node isolation attack by employing the same tactics used by the attack itself.Through extensive experimentation it demonstrates the proposed protection prevents more than95% of attacks and the overhead required drastically decreases the network size and it increasesuntil it is non-discernable. Lastly the main solution of this type is to extend the similar DDOS attacks on OLSR.DDOS attack, distracting application service reasonably todiminish the network resource, has occurred as a larger threat to network services, compared to the common DOS attack. Due to its high similarity to real traffic and much lower launching overhead than common DDOS attack, this attack type cannot be well detected or prevented by existing detection solutions. To identify DOS attack, propose a novel group testing (GT)-based approach deployed on servers which are back end, to find short detection delay and low false positive/negative rate.

Keywords- MANET, DDOS, OLSR, GT.

1. INTRODUCTION

MANET is acronym of Mobile Ad-hoc NETwork, which is a group of mobile devices that are able to communicate wirelessly with each other. Sending packets from one device to another isdone via a chain of intermediate nodes.A number of different routing algorithms exist for network packet transmission. For the most part these algorithms can be classified into two main categories: reactive routing and proactive routing protocols. In the case of proactive (tabledriven)protocol, for example, DSDV and OLSR every node constantly maintains a list of all possible destinations in the network and the optimal paths routing toit. Reactive protocols, such as DSR and AODV find aroute only on demand. Irrespective of routing algorithm, one of MANET's essentialrequirements of and a factor in its success is its ability ofhaving all nodes recognized by other participants, even inmotion.

These algorithms differ from the standard routing used inclassic networks due to frequent topology changes. A route between two nodes can be broken due to intermediate nodesthat dynamically change their position. Mobile nodes can join or leave the network at will, further influencing network connectivity. In this project review a specific DOS attack called nodeisolation attack and propose a new mitigation method.

Our solution called Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes.

Moreover, DCFM utilizes the samet echniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is consistent with general claim that OLSR functions best on large networks.

The identification of attackers can be much faster if can find them out by testing the clients in group instead of one by one. Thus, the key problem is how to group clients and assign them to different server machines in a sophisticated way, so that if any server is found under attack, can immediately identify and filter the attackers out of its client set. Apparently, this problem resembles the group testing (GT) theory which aims to discover defective items in a large population with the minimum number of tests where each test is applied to a subset of items, called pools, instead of testing them one by one. Therefore, apply GT theory to this network security issue and propose specific algorithms and protocols to achieve high detection performance in terms of short detection latency and low false positive/negative rate. Since the detections are me rely based on the status of service resources usage of the victim servers, no individually signature-based authentications or data classifications are required; thus, it may overcome the limitations of the current solutions.

2. RELATED WORK

Depth-first forwarding (dff).a data forwarding mechanism for Use in unreliable networks such as sensor networks and mobile Ad hoc networks with limited computational power and storage,Low-capacity channels, device mobility, etc. Routing protocols for These networks try to balance conflicting requirements of being Reactive to topology and channel variation while also being frugal In resource requirements.but when the underlying topology Changes, routing protocols require time to re converge, during Which data delivery failure may occur. Dff was developed to alleviate this situation: it reacts rapidly to local data delivery failures And attempts to successfully deliver data while giving a routing Protocol time to recover from such a failure. An extension Of dff, denoted as dff++, is proposed in this project, in order To optimize the performance of dff by way of introducing a More efficient search ordering . Advances in microcontroller and wireless technology, the concept of •\being online. is no longer exclusively reserved for computers, but expected also for phones, vehicles, televisions, refrigerators, utility meters, etc.Once routes to a destination have been found, they might become unusable, in a no predictable time-varying fashion: dynamic topology, presence of noise or interferences, low power supply in certain devices, unidirectional links, etc.

Mobile ad hoc networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Due to unique 18 characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET is a particularly challenging task compared to a conventional network. Early work in MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment.The main draw back of these approaches are that they cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

Mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network. survey of the main types of attack at the network layer, and then review intrusion detection and protection mechanisms that have been proposed in the literature. classify these mechanisms as either point detection algorithms that deal with a single type of attack, or as intrusion detection systems (IDSs) that can deal with a range of attacks. IDS needs a scalable architecture based on cross-layer design to detect these attacks effectively. surveyed and classified IDSs in MANETS based on their architecture and the addressed type of attack. A number of mechanisms for detecting black hole attacks.

The special network characteristics, such as limited battery power and mobility, make the prevention techniques based on cryptographic primitives ineffective to cope with such attack.Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails,some economic-based approaches can be adopted to alleviate theattack consequences by motivating the nodes cooperation. As a backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them.The main advantage of this scheme is its high detection accuracy that significantly reduces the number of false alarms. The security approaches that are solely based on symmetric-key cryptography are less robust and offer less security than asymmetric key cryptography, due to the higher probability that the shared keys being compromised. Main disadvantage is the induced overhead if the check process is repeated for each intermediate node replying to the RREQ.

The MDSR algorithm comprises The source node forwards the block of packet to the destination nodes once the packet reach the destination the probability of data reached is calculated if its value is greater than threshold value of packet loss then it initiates the gray hole detection procedure. The destination node begins the detection of the presence of malicious attacks in the source route using query request and mark it as suspicious nodes. The IDS nodes that are adjacent to the suspected nodes turn into promiscuous mode and hear whether the data packets are forwarded or dropped by the suspected nodes, if there is drop of packets then the node is isolated and the broadcast message send to all normal behavior nodes thus preventing the further attack.Many assumptions in the proposed work which is not applicable in real time environments such as all nodes can be similar in their physical properties such as transmission range, all nodes were authorized.

3. SYSTEM MODEL

The objectives of this project is to identify DoS attack, propose a novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an underlying framework against general network attacks.

DENIAL-OF-SERVICE (DoS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security . Traditional DoS attacks mainly abuse the network bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network. Consequently, several network-based defense methods have tried to detect these attacks by controlling traffic volume ordifferentiating traffic patterns at the intermediate routers .However, with the boost in network bandwidth and service types, recently, the target of DoS attacks has shifted from network to server resources and procedures themselves, forming a new DoS attack .
As stated in, by exploiting flaws in design and implementation, DoS attacks exhibit three advantages over traditional DoS attacks which help evade normal detections: malicious traffic is always indistinguishable from normal traffic, adopting automated script to avoid the need for a large amount of “zombie” machines or bandwidth to launch the attack, much harder to be traced due to multiple redirections at proxies. According to these characteristics, the malicious traffic can be classified into legitimate-like requests of two cases: 1) at a high inter arrival rate and 2) consuming more service resources.

The identification of attackers can be much faster if can find them out by testing the clients in group instead of one by one. Thus, the key problem is how to group clients and assign them to different server machines in a sophisticated way, so that if any server is found under attack, can immediately identify and filter the attackers out of its client set. Apparently, this problem resembles the group testing (GT) theory which aims to discover defective items in a large population with the minimum number of tests where each test is applied to a subset of items, called pools, instead of testing them one by one.

Therefore, apply GT theory to this network security issue and propose specific algorithms and protocols to achieve high detection performance in terms of short detection latency and low false positive/negative rate. Since the detections are me rely based on the status of service resources usage of the victim servers, no individually signature-based authentications or data classifications are required; thus, it may overcome the limitations of the current solutions.
The first requirement of the proposed method is that eachnode will only use information available to it, without relyingon any centralized or local trusted authority. Our technique does not actively verify the HELLO message, rather it checksits integrity by searching for contradictions between the HELLO message and the known topology. allow for loneMPR nominations, provided that no contradictions are found. Even in the face of contradictions, an MPR can be nominatedfor all 2-hop neighbors for which it is the sole access point.It cannot, however, be nominated as sole MPR for 2-hopneighbors that can be reached through other paths. assume that TC messages cannot be spoofed. justify this assumption due to the fact that bogus TCmessages do not preclude a legitimate (attacked) victim fromtransmitting a valid TC that contradicts the bogus one. Inessence, by publishing a fraudulent TC, the attacker disclosesthat he is attacking; allowing others to take preventive measures.A fake HELLO message is a much more cripplingattack, because it removes a victim from the network withoutits knowledge. Hence, DOS and network disruption due tofraudulent TC messages is outside the scope of this project.

3.1. Fictitious Setting Mechanism

In order to prevent nodes in the network from disseminatingfalse information about their connectivity to the others, setup a mechanism requiring each node to check whether anattack can be made through it. If such a lie is possible, thenode adds a fictitious node to the network, preventing anyonefrom claiming false connectivity to this fake node. That is,responsibility for correctness of the connectivity information isdelegated to the nodes themselves, as they must inhibit othersfrom using them falsely.The limitation mechanism for adding or removing fictitiousnodes is given by: 1) Each node v has to add a fictitious node when8z 2 ADJ2(v)9y 2 ADJ(v) such that the distance between y and z <3-hops.

2) Fv =2 ADJ(v).

3) New node z, advertises Fz by default, and only thencalculates rule 1.

4) Removing the fictitious node is done when (1) is false.

5) Examination must be performed periodically (every FICTITIOUS_CHECK_INTERVAL1).

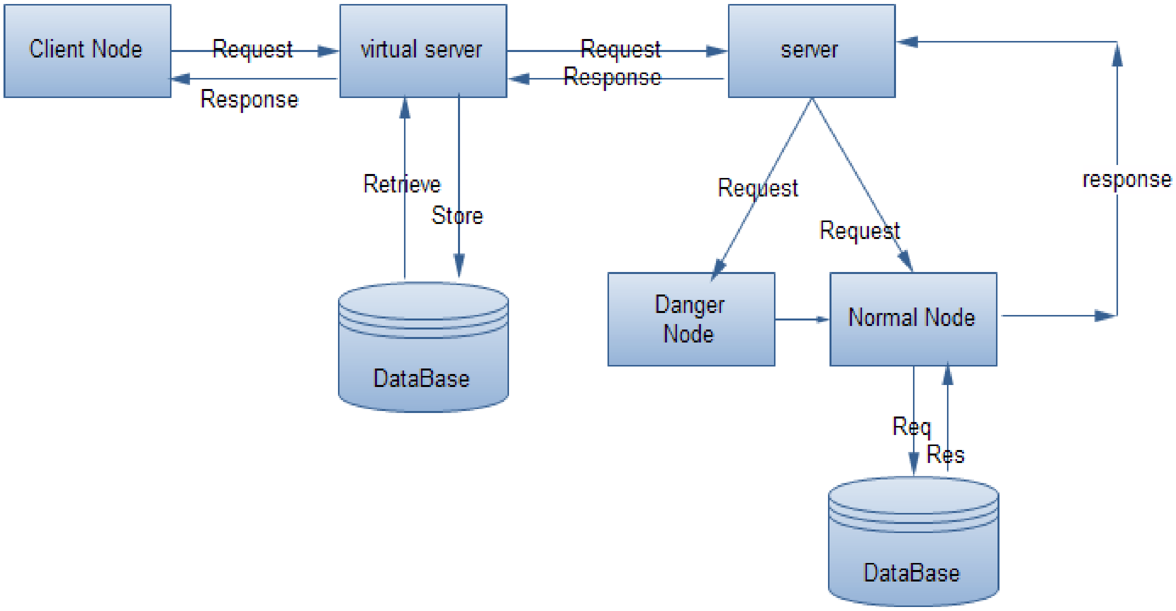
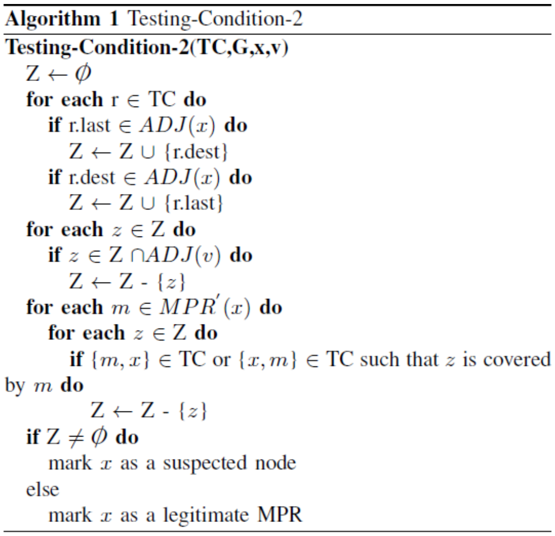


Fig.1. **System Architecture**



```
Algorithm 1 Testing-Condition-2
Testing-Condition-2(TC,G,x,v)
  Z ← $\emptyset$
  for each r ∈ TC do
    if r.last ∈ $ADJ(x)$ do
      Z ← Z ∪ {r.dest}
    if r.dest ∈ $ADJ(x)$ do
      Z ← Z ∪ {r.last}
  for each $z$ ∈ Z do
    if $z$ ∈ Z ∩$ADJ(v)$ do
      Z ← Z - {$z$}
  for each $m \in MPR'(x)$ do
    for each $z$ ∈ Z do
      if $\{m, x\}$ ∈ TC or $\{x, m\}$ ∈ TC such that $z$ is covered by $m$ do
        Z ← Z - {$z$}
  if Z ≠ $\emptyset$ do
    mark $x$ as a suspected node
  else
    mark $x$ as a legitimate MPR
```

Fig.2. Login Process DENIAL OF SERVICES

It may be possible to overwhelm the login process by continually sending login-requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond.When a user enters an incorrect username and/or password, the application should respond with a generic error message stating that the information entered was incorrect. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application. Whilst applications may handle authentication failure messages correctly, many still allow attackers to enumerate users through the *forgotten password* feature.

3.2. Group attacker modules.

The maximum destruction caused by the attacks includes the depletion of the application service resource at the server side, the unavailability of service access to legitimate user, and possible fatal system errors which require rebooting the server for recovery. assume that any malicious behaviours can be discovered by monitoring the service resource usage, based on dynamic value thresholds over the monitored objects. Data manipulation and system intrusion are out of this scope. That application interface presented by the servers can be readily discovered and clients communicate with the servers using HTTP/1.1 sessions on TCP connections. consider a case that each client provides a non spoofed ID, which is utilized to identify the client during our detection period. Despite that the application DoS attack is difficult to be traced; by identifying the IDs of attackers the firewall can block the subsequent malicious requests. The attackers are assumed to launch application service requests either at high inter arrival rate or high workload, or even both. The term “request” refers to either main request or embedded request for HTTP page. Since the detection scheme proposed will be orthogonal to the session affinity, do not consider the repeated one-shot attack mentioned in. further assume that the number of attackers d << n where n is the total client amount. This arises from the characteristics of this attack. Due to the benefits of virtual server s employee, this constraint can be relaxed, but keep it for the theoretical analysis in the current work.

3.3. Group testing modules

The classic GT model consists of t pools and n items (including at most d positive ones). This model can be represented by a t _ n binary matrix M where rows represent the pools and columns represent the items. An entry M[I, j]= 1 if and only if the I th pool contains the j th item; otherwise, M[I, j]= 0. The t-dimensional binary column vector V denotes the test outcomes of these t pools, where 1-entry represents a positive outcome and 0-entry represents a negative one. Note that a positive outcome indicates that at least one positive item exists within this pool; whereas negative one means that all the items in the current pool are negative. A detection model based on GT can be assume that there are t virtual servers and n clients, among which d clients are . Binary testing matrix M and testing outcome vector V. Attackers. Consider the matrix M t*n in Fig. 1, the clients can be mapped into the columns and virtual servers into rows in M, where M[I, j]= 1 if and only if the requests from client j are distributed to virtual server i. With regard to the test outcome column V, have V[i]= 1 if and only if virtual server i has received malicious requests from at least one attacker, but cannot identify the attackers at once unless this virtual server is handling only one client. Otherwise, if V ½i_ ¼ 0, all the clients assigned to server I are legitimate. The d attackers can then be captured by decoding the test outcome vector V and the matrix M.

3.4. Victim/Detection modules.

The victim model in our general framework consists of multiple back-end servers, which can be Web/application servers, database servers, and distributed file systems. do not take classic multitier Web servers as the model, since our detection scheme is deployed directly on the victim tier and identifies the attacks targeting at the same victim tier; thus, multitier attacks should be separated into several classes to utilize this detection scheme. assume that all the back-end servers provide multiple types of application services to clients using HTTP/1.1 protocol on TCP connections.

Each back-end server is assumed to have the same amount of resource. Moreover, the application services to clients are provided by K virtual private servers (K is an input parameter), which are embedded in the physical back-end server machine and operating in parallel. Each virtual server is assigned with equal amount of static service resources, e.g., CPU, storage, memory, and network bandwidth. The operation of any virtual server will not affect the other virtual servers in the same physical machine .There a sons for utilizing virtual servers are twofold: first, each virtual server can reboot independently, thus is feasible for recovery from possible fatal destruction; second, the state transfer overhead for moving clients among different virtual servers is much smaller than the transfer among physical server machines.

CONCLUSION

A novel technique for detecting application DOS attack by means of a new constraint-based group testing model. Motivated by classic GT methods, three detection algorithms were proposed and a system based on these algorithms was introduced. Theoretical analysis and preliminary simulation results demonstrated the outstanding performance of this system in terms of low detection latency and false positive/negative rate. This project is to apply group testing principles to application DOS attacks, and provide an underlying framework for the detection against a general case of network assaults, where malicious requests are indistinguishable from normal ones. For the future work, will continue to investigate the potentials of this scheme and improve this proposed system to enhance the detection efficiency. Some possible directions for this can be: The sequential algorithm can be adjusted to avoid the requirement of isolating attackers. More efficient d-disjunct matrix could dramatically decrease the detection latency, as showed in the theoretical analysis. A new construction method for this is to be proposed and can be a major theoretical work for another project.The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques. Even that already have quite low false positive/ negative rate from the algorithms, can still improve it via false-tolerant group testing methods. This error-tolerant matrix has great potentials to improve the performance of the PND algorithm and handle application DOS attacks more efficiently and improve this proposed system to enhance the detection efficiency.The sequential algorithm can be adjusted to avoid the requirement of isolating attackers.More efficient d-disjunct matrix could dramatically decrease the detection latency, as showed in the theoretical analysis. A new construction method for this is to be proposed and can be a major theoretical work for another project.The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques.Even that already have quite low false positive/ negative rate from the algorithms, can still improve it via false-tolerant group testing methods.

REFERENCES

1. C. E. Perkins and P. Bhagwat, ―Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers,‖ in Proceedings of the Conference on Communications Architectures, Protocols and Applications, ser. SIGCOMM '94. New York, NY, USA: ACM, 1994, pp. 234–244.
2. C. Perkins and E. Royer, ―Ad-hoc on-demand distance vector routing,‖ in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, Feb 1999, pp. 90–100.
3. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, ―Optimized link state routing protocol for ad hoc networks,‖in Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62–68.
4. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, ―Securing the olsr protocol,‖ in Proceedings of Med-Hoc-Net, 2003, pp. 25–27.
5. T. Clausen and P. Jacquet, ―RFC 3626 - Optimized Link State Routing Protocol (OLSR),‖ p. 75, 2003. [Online]. Available: http: //www.ietf.org/rfc/rfc3626.txt
6. D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, ―An advanced signature system for olsr,‖ in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ser. SASN '04. New York, NY, USA: ACM, 2004, pp. 10–16.
7. D. Dhillon, T. Randhawa, M. Wang, and L. Lamont, ―Implementing a fully distributed certificate authority in an olsr manet,‖ in Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, vol. 2, March 2004, pp. 682–688 Vol.2.28.