BALANCING LOAD ON DATA SHARING PROVIDED WITH PRIVACY

[1]Dr. C.Gunavathi , [2]N.Sugalya, [3]R.Vidhyarani, [4] D.Rameshraja
[1]Professor, Department of CSE, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India.
[2][3][4] Department of CSE, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India
Email:[1]sssguna@gmail.com, [2]sugalya14@gmail.com, [3]vidhyacse23@gmail.com, [4] rameshjetcn@gmail.com

***ABSTRACT* –** One of the major attacks to neighbor discovery is Wormhole Attack, in which malicious node's relay packets for two legislate nodes to fool them believing that they are direct neighbors. It seems that the merit kind of attack can enlarge the communication ranges, however, since it causes unauthorized physical access, selective dropping of packets and even denial of services, the wormhole attack is intrinsically a very serious problem especially in case of emergent information transmission.

This project proposes a wormhole attack resistant Secure Neighbor Discovery (SND) scheme, it is mainly regarding to directional wireless network. The SND scheme consists of three phases they are Network Controller (NC) broadcasting phase, the network nodes response/authentication phase and the NC time analysis phase. In the broadcasting phase and the response/authentication phase, local time information and antenna direction information are elegantly exchanged with signature-based authentication techniques between NC and legislates network nodes, which can prevent most of the wormhole attacks.

In the NC time analysis phase, the NC can further detect the possible attack by using the time-delay information from the network nodes. To solve the transmission collision problem in the response/authentication phase, we also introduce a novel Random Delay Multiple Access (RDMA) protocol to divide the RA phase into M periods, In which the unsuccessfully transmitting nodes randomly select a time slot to transmit. The optimal parameter setting of the RDMA protocol and the optional strategies of the NC are included. The application is designed using Microsoft Visual Studio .Net 2005 as front end. The coding language used is Visual C# .Net. MS-SQL Server 2000 is used as back end database.

Key words: Wormhole Attack, Secure Neighbor Discovery (SND), Network Controller (NC), Random Delay Multiple Access (RDMA).

INTRODUCTION

MAIN OBJECTIVES

- To reduce the power consumption in switching between the active and sleep mode of the nodes.
- To schedule the transmission time to the available neighbor nodes.
- To detect the malicious weight information provided by the nodes during the packet transmission.

SPECIFIC OBJECTIVES

- To extend the generic algorithm and implement the Weight Based Synchronization algorithm to find the winner slot to store the packet data.
- To extend the Weight Based Synchronization algorithm and implement the Future Peak Detection algorithm to avoid the inflation attack which is made by sending false maximum weight among the nodes.
- To extend the Future Peak Detection algorithm and implement the Randomized Future Peak Detection algorithm to synchronize all the neighbor nodes by using all the slots.

LITERATURE REVIEW

Load balancing plays a pivotal role in core routers as they need to handle multiple requests at a time. To achieve load balancing Multipath Switching Systems (MPS) are widely used. In this paper we built a prototype application which is a custom simulator that demonstrates the usefulness of FS scheme in terms of load balancing efficiency. The experimental results revealed that the FS scheme is effective in load balancing [1]. Load balancer allocates the work to the clusters of SIP server. The several load balancing algorithms for distributing Session Initiation Protocol (SIP) request to a cluster of SIP servers. The load balancer algorithm Transaction Least Work Left is used to allocate work to least values of the servers. It is combine knowledge of the SIP [2].

The onion router (TOR) allows to hide your identity various software under this categories are available that allows online anonymity. It doesn't allow network surveillance or traffic analysis to get tracked but most of these software [3]. Aggregation (by filtering source prefixes instead of individual IP addresses) helps reduce the number of filters, but comes also at the cost of blocking legitimate traffic originating from the filtered prefixes [4].

A protocol that supports the sharing of resources that exist in different packet switching networks is presented. The protocol provides for variation in individual network packet sizes, transmission failures, sequencing, flow control, end-to-end error checking, and the creation and destruction of logical process-to-process connections. We argue that by removing the unnecessary yoke of loss avoidance from congestion control protocols, by using Random Early Detection (RED) Detect incipient congestion [5]. Traffic characteristics and measurement objectives can change dynamically, rendering a placement of monitors suboptimal. It will not be the feasible solution to dynamically reconfigure measurement infrastructure. The problem is addressed by strategically routing traffic subpopulations over fixed monitors [6]. To compare our algorithms to several well-known approaches and present scalability results for up to 10 nodes. Our best algorithm, Transaction Least-Work-Left (TLWL), achieves its performance by integrating several features: knowledge of the SIP protocol, dynamic estimates of back-end server load, distinguishing transactions from calls, recognizing variability in call length, and exploiting differences in processing costs for different SIP transactions [7].

EXISTING SYSTEM

The existing system proposes a wormhole attack resistant SND scheme, which establishes the communications with signature-based authentication techniques, and achieves SND by utilizing the information of antenna direction, local time information and carefully designed length of the broadcast message.

Second, it introduces a random delay multiple access (RDMA) protocol to solve the transmission collision problem in the response/authentication phase when each node in the same sector does not have information of others and which cannot listen to the others' transmissions due to the limitation of directional antenna.

Third, it conducts extensive secure analysis and neighbor discovers time analysis to demonstrate the effectiveness and efficiency of the proposed wormhole attack resistant SND scheme.

DRAWBACKS OF EXISTING SYSTEM

- Synchronization among the nodes is not considered.
- The next transmission schedule for synchronization with neighbor node is not calculated.
- The suspicious node cannot be tracked in inflation attack scenario.

PROPOSED SYSTEM

The new system eliminates the problem by calculating the transmission schedule using the weighted information based on the proposed algorithm steps. In regarding to addition, synchronizing all the neighbor nodes which belong to various clusters is a must to attain the stable state of the network.

The proposed system present the techniques for synchronizing nodes that periodically broadcast content and presence updates to co-located nodes over an ad hoc network. Instead of aligning duty cycles, the new algorithms synchronizes the periodic transmissions of nodes. This allows nodes to save battery power by switching off the network cards without missing updates from their neighbors. Several novel attack classes are proposed to show that they are able to disrupt synchronization even when launched by a single attacker.

To avoid the drawbacks in the existing system, mainly when the weight details provided by the neighbor nodes are been considered as false, a system which identifies the weight by not using the packet data and finding the weight based on the weight in the slots is required to identify the winner slot efficiently. Hence the new system is being proposed. In the new system, synchronization occurs very quickly (order of minutes instead of hours). For application requirements and specific ecosystem, the needed all nodes to receive updates frequently and reliably, the scheduled rendezvous based wake-up approach was the obvious choice. The suspicious node can be tracked easily since it does not satisfy the node behaviors of neighbor nodes.

.NET Framework

The .Net framework consist of web forms, windows forms and console application that pertain the presentation layer of an application. Window form is a language –independent from engine that brings the drag and drop design feature of Visual Basic to all .Net enable language. Web form brings the drag and drop design and event drive architecture to web design interfaces, implementation a programming model.

.NET framework class Library:

The .Net class framework consists of a class library that works any .NET language. The class library is built on the object oriented nature of runtime. It provides classes that can be used to accomplish a range of common programming tasks such as string management, data collection, and database connectivity and file access.

Common Language Runtime (CLR):

It is a heart of the .Net framework. The core of the CLR is an execution engine that loads the executions and manages code that has been compiled into intermediated byte code format called Microsoft Intermediate Language (MSIL). The byte code is not interpreted. It is compiled to native binary code before execution by Just-In-Time (JIT) compilers built into the CLR. CLR can execution programs written in any languages. The CLR provides functionality such as exception handling, security, debugging and version support to any language that targets.

Common Type System:

It supports a variety of data types and found in most programming languages and therefore calling from one language to other doesn't require type conversion. C# is specially designed for the .NET platform, build .NET programs in a number of other language including C++, and Visual Basic.

Overview of ADO.NET

ADO.NET is an evolution of the ADO data access model that directly addresses user requirements for developing scalable applications. It was designed specifically for the web with scalability, statelessness and XML in mind. ADO.NET is new programming model built upon the .NET Framework, sharing a common type system, design patterns and naming conventions.

The stated goals of ADO.NET are to:

- Provide a disconnected data architecture in addition to support the connection operation.
- Integrate tightly with XML.
- Interact with a variety of data source though a common data representation.
- Optimize data source access.

It is connection opened only when it's long enough to perform a database operation such as to select and update. The rows are read into a dataset and work and then work with connected to the data source.

Transmitting an ADO.NET dataset between applications is much easier than transmitting a record set. To transmit data in ADO>NET, a dataset is used which can transmit an XML stream. ADO.NET is based on an XML format, there is no restriction on data types. Thus, the component sharing the dataset can use rich set of data types they used ordinarily.ADO.NET does not require data type conversions and minimized data transmitted. ADO.NET dataset using XML, firewalls can allow datasets to pass. Memory resident data representation Data Table objects.

C# Language:

C# is a Microsoft's new language designed for its new platform ".NET". It is fully object oriented language like java and is the first component-oriented language. Because it contains integral supports for writing the software components. C# is designed for building robust, reliable and durable components to handle real world application. The C# language specification stated the objectives and features of C#

It is simple, modern, general purpose and object oriented programming language. This provides a support for the software analysis principles such as strong type checking, array bounds checking, detection of attempts to use uninitialized variables and automatic garbage collection. It is useful for developing software components which are suitable for deployment in the distributed environments. This supports internationalization.

Characteristics of C#:

Garbage Collection**:** the memory management feature leads all managed objects. Garbage collection is a feature .NET. The C# uses it during the runtime.

Indexes:

C# has indexes which help to access value in a class with an array like syntax programs.

Exception Handling: .NET standardizes the exception handling across languages. C# offers the conditional keyword to control the flow and make the code more readable.

Versioning:

C# programming supports this versioning. The .NET solves the versioning problem and enables the software developer to specify version dependencies between the different pieces of software.

Extensive Inter-operability: All enterprise software application can be managed easily by type safe environment. This extensive inter-operability makes C# which is the obvious choice for the software developers.

CONCLUSION

This proposes now several algorithms for synchronization mechanisms. However, the use of random values in winner slot calculation does not provide cent percent accuracy. So the extension of proposed algorithms with a new algorithm is required for highly efficient communication between nodes.

If the application is tested with real mobile nodes, then it can assist the further proceeding of the algorithm implementation practically.

In addition, if the experimental application is designed based on web, then it can access the platform independently and the usage will be increased. The new system is designed such that all those enhancements can be integrated with current modules easily with less integration work.

REFERENCES

[1]P.Poojitha, G.Suhasini "Load-Balancing Multipath Switching System with Flow Slice" PP. ISSN: 2231-2803. Proc. International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 4 –Nov 2013

[2]S.Tharani,Balika.J.Chelliah,Dr.J.Jagadeesan"An Efficient Server Load Balancing using Session Management"ISSN 2319 – 4847.prov. International Journal of Application or Innovation in Engineering & Management (IJAIEM)- Volume 3, Issue 2, February 2014

[3] Nakil Komal Mahendrakumar, Sonkar Shriniwas K" Analysis of Cell-Counting Based Attack Against Tor" ISSN 2250-2459, ISO 9001:2008 Certified Journal.prov. International Journal of Emerging Technology and Advanced Engineering-Volume 3, Issue 5, May 2013

[4] Fabio Soldo, IEEE Student Member, Katerina Argyraki, IEEE Member, and Athina Markopoulou, IEEE Member" Optimal Source-Based Filtering of Malicious Traffic"

[5] K.K. Nikhil, G. Sunil Santhosh Kumar" packet loss control using tokens at the network edge" ISSN: 0975 – 6760.proc. Journal of information, knowledge and research in computer engineering-vol – 02, issue – 02, nov 12 to oct 13

[6] S.Priya, S.Pushpac" Measurouting Approach for Flow Utility in Routing Assisted Traffic Monitoring " ISSN: 2278-3075.proc. International Journal of Innovative Technology and Exploring Engineering (IJITEE)- Volume-2, Issue-4, March 2013

[7] Hongbo Jiang, Arun Iyengar, Erich Nahum, Wolfgang Segmuller, Asser N. Tantawi, Charles P. Wright," Design, Implementation, and Performance of a Load Balancer for SIP Server Clusters"ISSN: 1063-6692.prov. ieee/acm Transactions on Networking-2012