International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-5, June 2012

Comparison of Security Algorithms in a Distributed Monitoring Environment

Kaushik Sanganabhatla

Abstract: ***In a Real time wireless environment like WIFI, we send the data in the form of packets from one location to other. While sending the data to destination safely, we maintain some security algorithms for the confidentiality of the data. We use the knowledge of many pre- existing algorithm mechanisms for the smooth flow of the data packets in a timely & secured manner. Here, the main objective is to compare the various security algorithms in ganglia distributed monitoring system. The research stimulates that comparing the constant algorithms (1-point/minimal & 10-point/maximal) with the variable (optimal) algorithms. From these it can be concluded that the CPU memory usage is less in optimal algorithm in terms of against high load, bytes- in, bytes-out characteristics.***

Key words: 1-point or minimal, 10point or maximal, optimal algorithms and ganglia.

I. INTRODUCTION:

A computer network is a group of computers that shares information across wireless or wired technology. Computer networking requires two computers, a protocol and the hardware to connect them. Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. Sometimes it's also referred to as WiFi network or WLAN [10]. You can connect computers anywhere in your home without the need for wires.

Here is simple explanation of how it works, let say you have 2 computers each equipped with wireless adapter and you have set up wireless router. When the computer sends out the data, the binary data will be encoded to radio frequency and transmitted via wireless router. The receiving computer will then decode the signal back to binary data.

The two main components are wireless router or access point and wireless clients.

If you have not set up any wired network, then just get a wireless routerand attach it to cable/DSL modem. You then set up wireless client by adding wireless card to each computer and form a simple wireless network. You can also cable connect computer directly to router if there are switch ports available.

If you already have wired Ethernet network at home, you can attach a wireless access point to existing network router and have wireless access at home. Nowadays, people can access to the various wireless technologies like WIFI, wireless internet at schools, cafeteria's, university, Restaurant, and even in travelling & perform various e-commerce applications.

Wireless networks can be easily attacked by computer viruses, worms, spy wares, and similar threats. Damage or destruction of the computer system led's towards destruction of data, hostile use of sensitive data, or damage to the organization's reputation.

So, Computer security is required because most organizations can be damaged by hostile software or intruders.

II. WIRELESS OPERATING MODES:

There are many types of 802.11 wireless standards [6] that can be used. For example 802.11a, 802.11b and 802.11g are three popular wireless communication standards.

A. 802.11a:

802.11a is not popular due to the slow availability of the 5 GHz components needed to implement products by vendor, more expensive cost The higher frequency also makes 802.11a signals have more difficulty to penetrate walls and other obstructions. It is usually found on business networks.

B. 802.11b:

The IEEE 802 committee extended to create an 802.11b standard. It became popular due to low setup cost and bandwidth support up to 11Mbps in the 2.4GHz S-Band for Industrial, Scientific, and Medical (ISM) frequency range.

C. 802.11g:

802.11g supports bandwidth up to 55Mbps in the 2.4GHz band. 802.11g use the same radio frequency (2.4GHz) to transmit data over the airwaves. 802.11g also provides better security features, such as WiFi Protected Access (WAP).

D. 802.11n:

802.11n can provide bandwidth up to 600Mbps, or 10 times faster than 802.11g.

802.11 standard that supports much higher bandwidth, but it's more expensive when we compare to 802.11g products.

In order to perform our experiment in WIFI we need to know all this things.

III. ALGORITHMS

The security algorithms [12] mainly consist of two constant packet scheduling algorithms (1-point or minimal algorithm and 10-point or maximal algorithm) and variable security Algorithm or optimal algorithm.

Manuscript published on 30 June 2012.
***** Correspondence Author (s)
Kaushik Sanganabhatla*, M.Tech Computer Science & Engineering, University College of Engineering, Osmania University Campus, Hyderabad, India.

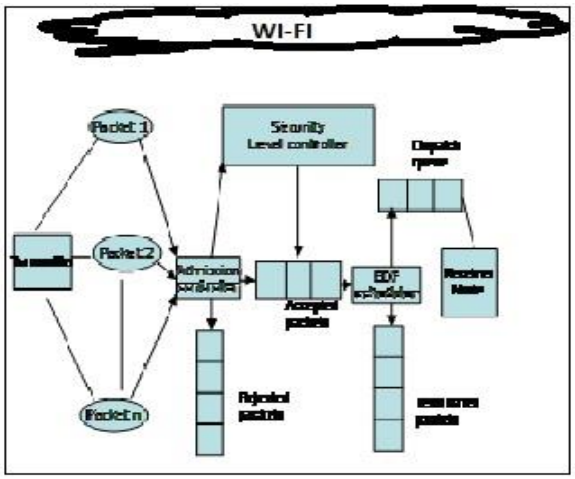

Figure 1: The base architecture of 1-point,10-point & optimal algorithms.

Depending upon the above architecture, all the security algorithms are designed. We are transmitting the data in the form of packets between two nodes in a wireless network (WIFI). Here, nodes mean transmitter & receiver. The function of the Admission Controller [7] is to determine whether incoming packets can be accepted or not. The Security Level Controller aims at increasing security levels of real-time packets residing in the Accepted queue that can be finished before their deadlines. The EDF scheduler makes use of the Earliest Deadline First policy to schedule admitted packets in which security levels are maximized by the Security Level Controller.

DESCRIPTION:

We assume that each packets have deadline[1] and each packet [2] is independent of one another. Packet P is represented as a vector (N,ST,ET,DL,SV). Here N initializes the serial number of the packet, ST represents the starting time of the packet, ET represents the ending time of the packet, DL means the Deadline of a packet & SV tends to the Security Level value of the each packet. We assume that each packet is assigned a security level SV measured as a in the range from 1 to 10, where 1 as lowest and 10 as highest levels of security. Although wireless network devices are unable to determine security levels, but here straight forwardly derived from the security applications [11].

If the deadline of the packet can be met, the packet will be admitted in the accepted queue. Otherwise, the packet will be dropped and placed in the rejected queue. The following constraint shows whether the packet is equipped to meet its deadline.

The difference of Ending Time (ET) & starting time(ST) is known as mean time(MT). If the mean Time (MT) is less than or equal to the Deadline (DL). It means that the packets with earlier deadlines will be processed first. The algorithm initializes the security levels of all packets depending upon the security algorithm.

A. 1-point or Minimal Algorithm:

The Admission Controller intentionally selects the lowest security level i.e. SV=1 for each coming packet. Therefore, there is no restriction & the guarantee delivery of packets is improved. But, any how we check the load, usage, bytes-in & bytes-out.

B. 10-point or Maximal algorithm:

The Admission Controller chooses the highest security level i.e. SV=10 for each accepted packet. As a security value is high so, there may be a less chance of guarantee delivery due to its restrictions.

C. Optimal Algorithm:

There are same Key components similar to that of 1-point or 10-point algorithms. But, the security values are variable which can be between the range of 1 to 10 values. If the security value (SV) is below 5, then we need to add 5 to the previous value.

For example, the SV value of 2nd packet is 2 then add 5 to it, becomes 7. However, you may get doubts that how can us increase directly the security value of a packet. But, this is an assumption based upon it we are experimenting.

IV. IMPLEMENTATION

We are implementing it under Wi-Fi network. It consists of 3 transmitters & receivers. Firstly, we take minimal algorithm & perform its execution then sending to receiver. Simultaneously, we execute the maximal & optimal algorithms. Then all this algorithms should be monitored in ganglia.

A. Ganglia Monitoring System:

Ganglia is a scalable distributed monitoring system for high performance computing systems such as clusters and Grids. It leverages widely used technologies such as XML for data representation, XDR for compact, portable data transport, and RRD tool for data storage and visualization. The implementation is robust, and is currently in use on over 500 clusters around the world. Ganglia is also used by top giants like facebook, orkut, etc. for monitoring the performance in daily, weekly, monthly, quarterly, annual basis. There are currently three classes of distributed systems where Ganglia are being used: clusters, Grids, and planetary-scale systems.

This approach [1] offers several advantages including automatic discovery of nodes as they are added and removed, no manual configuration and symmetry in that any node knows the entire state of the cluster.

Ganglia is currently deployed on Clusters: Clusters are characterized by a set of nodes. In these systems, nodes are frequently homogeneous in both hardware and operating system, the system is managed by a single administrative entity.

B. Ganglia Architecture:

Ganglia [4] is based on a hierarchical design targeted at federations of clusters. Ganglia follow its own structure for implementation. It allows the user to remotely view live or historical statistics (such as CPU load, Memory Usage, Bytes-in & Bytes-out of network utilization) for all machines that are being monitored. Each cluster consists of two services gmond & gmetad.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Ganglia monitoring daemon (gmond) specifies that each node monitors its local resources and sends multicast packets containing monitoring data on a well-known multicast address whenever significant updates occur. Each node cluster's state is easily reconstructed after a crash.

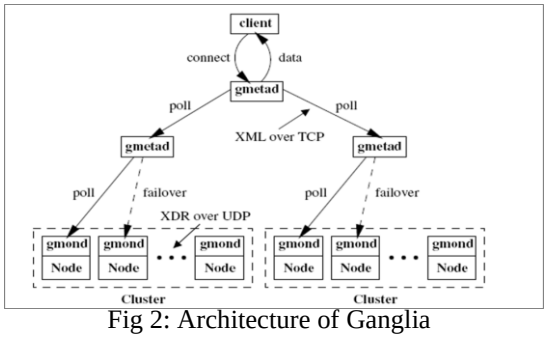

Fig 2: Architecture of Ganglia

Ganglia federate multiple clusters [5] together using a tree of point-to-point connections. Ganglia Meta daemon (gmetad) specifies multiple cluster nodes for each leaf to handle failures. Monitoring data from both leaf nodes and aggregation points is then exported using the same mechanism, namely a TCP connection to the node being polled followed by a read of all its monitoring data.

V. OBSERVATIONS & RESULT

Observation and comparison of all the 3 algorithms:

Observed Memory Usage for Minimal, Optimal and Maximal algorithms

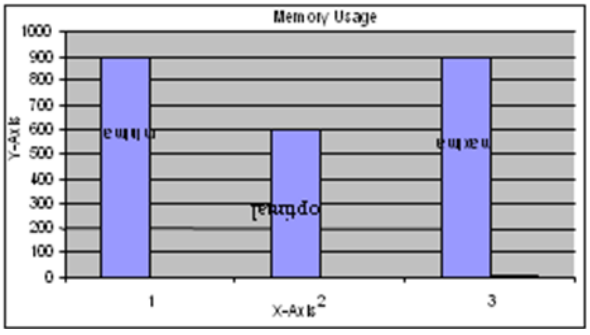

Fig 3: Graph representing the cpu memory usage.

Graph Observed Load for Minimum, Optimal and Maximal algorithms

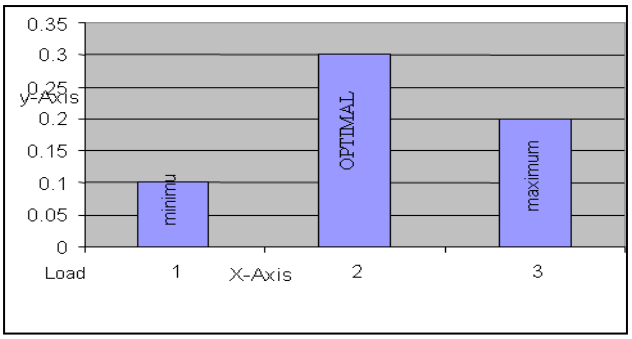

Fig 4: graph describing the Load

Observed Bytes-in for Minimal, Optimal and Maximal algorithms.

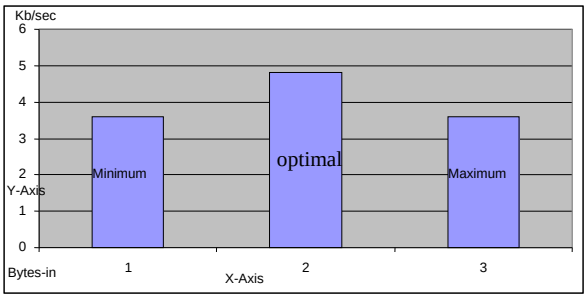

Fig 5. graph describing the Bytes-in

Observed Bytes-out for Minimum SPSS and Maximum algorithms.

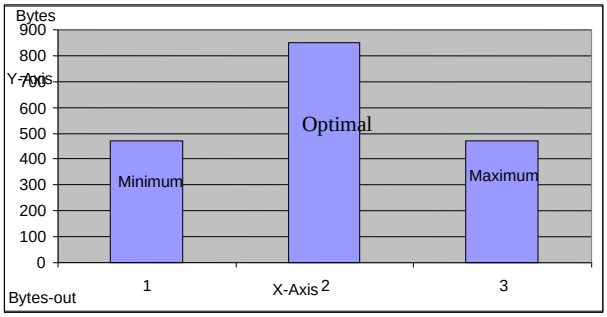

Fig 6. Graph describing the Bytes-out

When we take the performance of all the algorithms together the following can be observed.

1. In the case of CPU Memory Usage of SPSS algorithm is 600Mb when compared with the minimum (900Mb) and maximum (900Mb) algorithms.
2. Even with the high Load of 0.3 the SPSS Algorithm can perform less cpu memory usage than the minimum and maximum algorithms.

VI. CONCLUSION

The simulation experiments to evaluate the performance of our algorithm. Experimental results show that compared with two baseline algorithms (Minimum and Maximum Algorithms), the proposed algorithm can substantially improve both quality of security and CPU memory usage is less than minimum and maximum algorithms under a wide range of workload characteristics

The results proved to be satisfactory.

REFERENCES

[1] The ganglia distributed monitoring system: design, implementation, and experience Matthew L. Massie Available online 15 June 2004
[2] Improving Security of Real-Time Wireless Networks through Packet Scheduling by Xiao Qin, Mohamed Alghamdi in IEEE Transaction on wireless communication, VOL.7, and NO. 9, September 2008.
[3] Dynamic Task Scheduling with Security Awareness in Real-Time Systems by Andrew Sung in High Performance Computing and Networking, Vol. 1, Nos. 1/2/3, 2004
[4] Integrating Intelligent Anomaly Detection Agents into Distributed Monitoring Systems by German Florez-Larrahondo in Journal of Information Assurance and Security 1 (2006) 59–77.
[5] Job oriented monitoring of clusters by vijaya lakshmi in IJCSE.
[6] 802.11 security issues and solutions by D.M.Garge in IJCSC Vol. 2, No. 2, July-December 2011, pp. 587-591
[7] S. Lu, V. Bharghavan, and R. Srikant, "Fair scheduling in wireless packet networks," IEEE Transaction Networking Aug 1999.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[8] Text book**:** The complete reference "Network security" by Roberta Bragg and Keith strassberg**.**
[9] GradyBooch, Object oriented Analysis and design with applications, the benjimin/cummings, 1994.
[10] T. Karygiannis and L. Owens, IEEE journal on" wireless network security 802.11, Bluetooth and Handheld Devices".
[11] Scheduler based qos analysis by kumaran sharma IJRTE 2009.
[12] SPD (Static Priority with Deadline Considerations) Packet Scheduling Algorithm for achieving better QoS by Tamer Dag in Third International Conference on Networking and Services(ICNS'07) IEEE2007.

Kaushik Sanganabhatla has received M.Tech in Computer Science & Engineering from University College of Engineering Osmania University Campus, Hyderabad, India in January 2011, & B.Tech in Computer science & Engineering from Jawaharlal Nehru Technological University, Hyderabad, India in June 2008. His Area of Interest include Network Security, Grid Computing, Java. He Secured all India GATE Rank/Score: 373 with 93.70%.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)