Smart Home Network Monitoring and Troubleshooting System

Debajyoti Pal
King Mongkut's University of Technology Thonburi
19 PUBLICATIONS 23 CITATIONS

Smart Home Network Monitoring and Troubleshooting System

Debajyoti Pal
Assistant Professor
Camellia Institute of
Technology
Kolkata: 700129

ABSTRACT

The complexity of home networks has evolved to a greater level of sophistication and complicacy in the recent times comprising of heterogeneous components like at least two computers, web-enabled high-definition television sets, net-enabled blue ray disc players, iPods and many other such devices. Troubleshooting such a sophisticated *smart home network* in case of a malfunction by the novice end users seems to be very demanding. The paper proposes a Smart Home Network Monitoring System that provides a *centralized, general-purpose, automatic and convergent logging facility* with the purpose to auto-detect and possibly correct all such failure issues by having a well-defined set of *adaptive and incremental rule engine* that needs to be applied to the entire network in general. Logging of all *events* that happened *before* trouble appeared may give a greater insight and hence help in providing an effective and permanent troubleshooting mechanism. This paper also reports the initial experience of deploying such a facility.

General Terms

Computer networks and configuration.

Keywords

Smart Home Network Monitoring System, General-purpose logging facility, Adaptive and Incremental Rule-Engine, Event, Troubleshooting.

1. INTRODUCTION

Penetration of cheap broadband service in the past few years has lead to a surge in the home networking environment and subsequently the problems associated with it are becoming well-known. The ultimate goal of providing an integrated multimedia entertainment service has resulted in the emergence of smart home networks consisting of a number of sophisticated yet complex products like laptops, HDTV, Blue-ray disc players, tablets, etc that have ultimately created a plethora of problems for the ultimate home users. In fact the problems that plague the smart home networks though simple are a cause of great confusion and frustration among the end users because of their lack of knowledge and expertise [1, 2, 3]. Misconfigured home networks are a great deal of concern from the security point of view also because they serve as attractive trap-doors for external attackers to exploit. The causes for home network failure can be many and thus tools and logging facilities that enable us to automatically monitor, record, detect and correct such issues will be welcomed.

Continuous monitoring and logging of home network traffic (both inward and outward) can be helpful to provide an insight to the problems that arise in such a network. Specifically what event(s) led to the malfunctioning of the home network might come into limelight by maintaining such a log and can come to be handy in designing an automated, adaptive, and incremental self-diagnostic rule matching system(engine).

Packet-monitoring tools like *tcpdump, Wireshark, Kismet,* etc helps us to monitor and log all the incoming and outgoing network traffic. All of them however suffer from the same drawback of being tied down to one specific host at a time. Further, in most of the homes presence of a NAT enabled router/gateway for establishing an Internet connection to the ISP server complicates the issue in the sense that it renders the outward traffic monitoring useless. Also due to being tied down to one specific host, multiple tools need to be present one for each host that is a part of the smart home network.

This clearly gives rise to redundant data that serves as a bottleneck for the bandwidth which is shared between the different active devices.

In this paper we propose a centralized, general-purpose, automatic, convergent logging facility that serves as a basis to auto-detect and correct all possible smart home network failures. Since we used Wireshark as the packet monitoring tool, hence a centralized logging facility is required so as to ensure that redundant data flow and hence bandwidth clogging is minimized. Thus the home network implies the presence of client/server architecture which ensures that all the incoming/outgoing traffic is forced to pass through the centralized device that houses the packet monitoring tool. The logging platform is a general purpose one because not only does the packet monitoring tool we deploy operating system neutral but it also supports a wide variety of network protocols from the application, transport, network and data-link layers and of the TCP/IP stack. The logging facility is automatic because the packet monitoring tool at all times is running in the background and storing the events in a specified location of the storage disk. When a particular limit of the disc usage space is reached the recorded events are transferred to another secondary storage medium. The overall reliability of the system is increased by having the idea of primary/secondary storage in the event of primary storage failure. The centralized architecture that we follow automatically forces the entire system to be a convergent one because traffic from all possible locations are ultimately redirected to a centralized server that we already discussed.

The aforesaid facility has got a close resemblance with a typical “Black-box” present in the aircrafts and we refer to the system that houses the monitoring, logging and troubleshooting facility as the Smart Home Network Monitoring System (SHNM).

The outline of the paper is as follows. Section 2 describes the configuration and functionality of our SHNM system. Section 3 deals with the potential applications of such a system. Section 4 deals with the specific requirements and the challenges that can be faced by the system. Ultimately Section 5 gives the detail of our experimental test bed and the scope of future work.

2. SHNM SYSTEM CONFIGURATION AND FUNCTIONALITY

The place of deployment of the SHNM logging facility is of utmost importance. We follow the typical client/server architecture model[4] wherein a single system houses the SHNM facility and all the outgoing or incoming network traffic of any kind must flow through it. Such a scheme has been shown in the Figure 1 below.

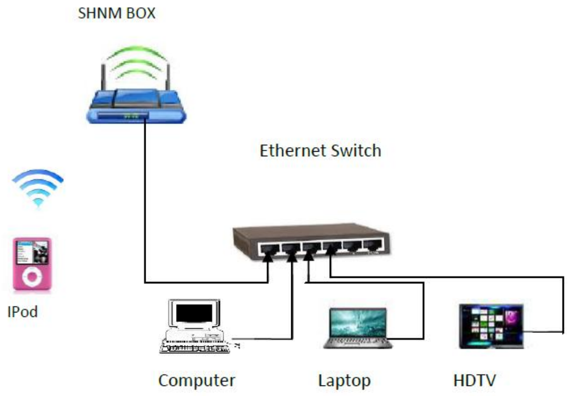

Figure 1

The configuration has provision both for wired as well as wireless devices. Since the total number of active network points can go well beyond 5 very easily we choose a 10 port Ethernet switch for the wired section which in turn is connected to one of the Ethernet ports of the SHNM system. Wireless support is also provided by the SHNM system directly in the form of IEEE 802.11a/b/g/n standards. Although home networks with a more complex configuration can do exist, but we assume ours to be a sufficient one for at-least a couple of years to come by.

Figure 2 depicts the overall SHNM system functionality.

As shown the SHNM system can be subdivided into 4 blocks namely:

i) Monitoring Block- It actually houses the packet monitoring software like Wireshark which is responsible for capturing all the home network data that are being generated and subsequently transmitted.

ii) Data Storage and Housekeeping Block- This block is responsible for storing all the packets that are being sensed by the Monitoring Block. Each and every packet is opened up and depending upon its contents a pre-defined rule-set is applied and the packets are transferred to a proper Event Generation Block.

iii) Event Generation Block- It actually can be subdivided into the following sub-blocks:

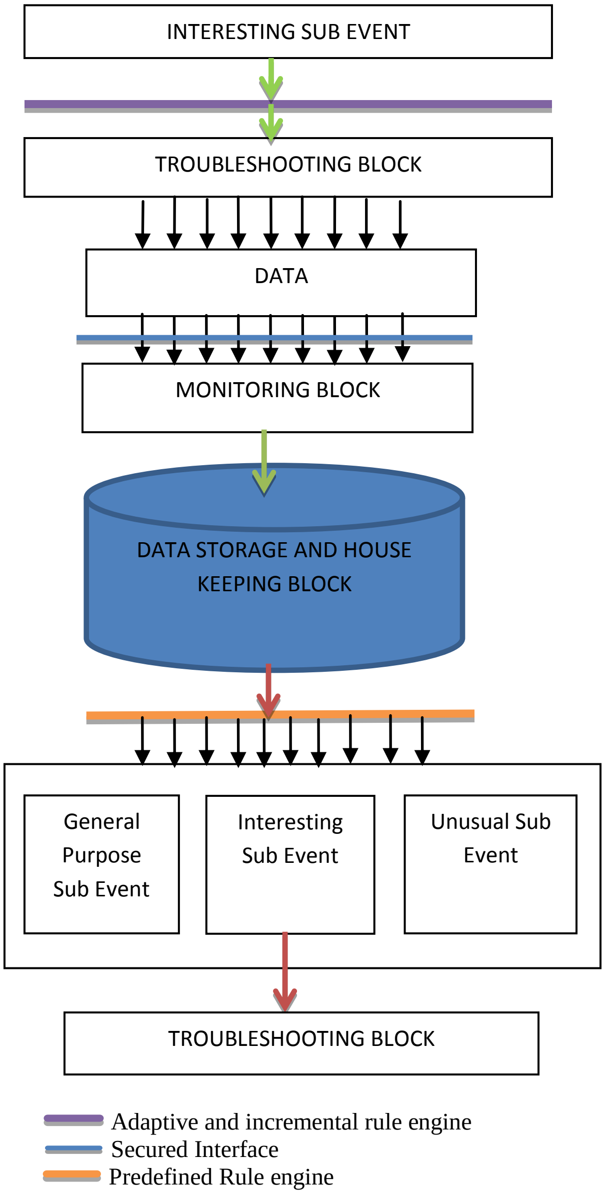

Figure 2.

a) General-Purpose Event Sub-Block which contain the logs of all the incoming and outgoing network traffic under normal and healthy network operating conditions (i.e. no network malfunction).

b) Unusual Event Sub-Block which contains the logs of some rare network traffic like a new MAC address appearing for the first time, or modification of the configuration settings of a file that is rarely touched.

c) Interesting Event Sub-Block which contains the logs of certain filtered network traffic that might be attempting to update an operating system, updating some antivirus software or searching for device driver software's for a newly installed piece of hardware (maybe like a graphics card) or any other such related items.

iv) Troubleshooting Action Block- It is this block that has access to the Interesting Event Sub-block and is of prime importance. It houses specialized application program that takes appropriate troubleshooting measures if such a condition is detected. Thus this sub-block should obviously have access to all the sensitive user-data also that might pose to be a security threat or a breach of privacy. Hence the interface that is used by this sub-block to access the user-data should be done through a secure channel as depicted by a dotted line in Figure 2.

The primary application of the SHNM system is to provide support for troubleshooting and diagnosis when some things fail on a smart home network. If the SHNM system is widely adopted then such a service might be provided by a third party provider or by the ISP itself as a value added service on a chargeable basis.

3. APPLICATIONS OF SHNM SYSTEM

In this section we consider some applications of our SHNM System.

i) Automatic Troubleshooting and Future Prediction- This obviously is the prime reason to have our SHNM system in place. Studies by Sheehan et al shows that end-users often seek online help to troubleshoot problems of their home network that they are facing[5]. Gathering the knowledge about millions of such end users spread all over the world we could easily produce a list that consists of the most commonly occuring home networking problems[6]. Thus the key to success is to both learn and share any new information with everybody else on the community as and when it appears. So, by collaborating the experiences from different such households the troubleshooting block rule engine can be made to adapt itself to such changes and consequently update its own rule engine. Given a considerable period of time our SHNM System would gradually evolve to an automated Expert System wherein, it might suggest for example, a particular brand of network connected HDTV's creating some sort of a network configuration problem based upon the experience of other households. Thus, given an existing smart home network it can give a suggestion to the users before buying about the best possible alternatives of devices that are available in the market and which are compatible with their own home network thereby ensuring a quality and hassle-free service.

ii) Ensuring Quality of Service(QoS) in terms of Internet Speed- Poor Internet speeds are a common cause of concern in almost every household. It can be due to a improperly configured network or due to policies set forward by the ISP itself. To detect situations wherein a user's ISP is the cause of performance degradation (relative to speed) Mukarram Bin Tariq *et al* have developed the Network Access Neutrality Observatory (NANO), which collects network-flow statistics from different households and attempts to isolate the cause of such performance degradations based upon a statistical model[7]. Thus, this opens up an opportunity to intermix the NANO agent with our SHNM system so as to improve its intelligence to understand the reasons of poor internet speeds if any and hence take appropiate measures.

iii) As a means to improve Network Security- Intrusion Detection Systems, antispywares, antivirus softwares and other network security algorithms depend heavily on their ability to collect different types of relevant data from as many sources as possible to keep themselves updated to the latest available threats[8, 9, 10]. Modern day scenario presents us with a very dangerous situation where the attackers could well be present in a smart home network as ours. The problem is even more complicated because different home networks may be subscribed to different ISP's and generally they work in isolation to each other. Thus a collaborative SHNM system should be in place wherein the SHNM systems from different home networks interact among themselves, sharing the data they have with the sole aim of detecting any possible new vulnerabilities arising out of such network traffics.

4. SPECIFIC REQUIREMENTS AND CHALLENGES FACED BY THE SHNM SYSTEM

i) Issue of privacy and its legal implications- It is evident by this time that in order to ensure effective troubleshooting, SHNM systems from various homes should inter co-operate among themselves. In fact collecting, sharing and using the information about the events occurring in people's home networks is more challenging than the same prospects in the enterprise or service-provider networks [11]. But in doing so we risk sensitive user informations and their personal preferences like the type of websites visited, personal credit card informations and so on to be at stake. Obviously, no user would ever want any outsider to have a see into the daily happenings of their household which should be kept as a secret. But in doing so the very basic concept of collaborative information collection mechanism would be violated. To further complicate matters in a country like India the Information Technology Act poses a hefty penalty or imprisonment for upto a few years on the ISP's who violate the privacy of their customers.

Thus the only solution that can be provided is to keep the SHNM System within the premises of a household only and to let the user of such a smart home network make a choice about which information is to be shared and which is to be not. Although it might sound to be a conservative approach, but right at this point of time it is the only best possible alternative available. Signing of a customer agreement form between the service provider and the customer may also be feasible solution.

The concept of automatic operating system software updates will work well with the SHNM system too given their widespread acceptance. In that case the SHNM system which is present in the household would regulary contact a centralized server of the service provider providing the SHNM service and keep the smart home network up to date.

ii) Storage Limitations- The problem of limited storage space is a very important one. The configuration that we used to test the system consisted of a modest 320 GB hard disk drive. Experiments revealed that for a full day of heavy Internet usage(consisting of 3 movie downloads, browsing the Internet and some e-mail exchanges) roughly 3 GB of disk space was utilized for storing the necessary records. This combined with the live streaming features being used on the HDTV's took up another 1 GB. Thus the entire disc space would be consumed in no more than 3 months. Hence periodic removal of the stored data to some offsite network storage device should be done at regular intervals. For example, data transfer from the SHNM system to any offsite network storage device can be scheduled at midnight of Sunday every week.

iii) Reliability Issue- The SHNM system we described should be robust and reliable. Specifically it should be immune for an acceptable period of time to power failures, or certain hardware configuration changes in the machine it is housed in. The design should be such that, in the event of any hardware failure the loss of log data should be minimum.

5. EXPERIMENTAL TEST BED AND SCOPE OF FUTURE WORK

We have implemented an initial prototype of the SHNM system as a tool to understand what exactly goes on in a home network. Our prototype design is based upon an Intel based system running Windows 7 Home Premium Edition as the operating system. Further a software called CCProxy is also installed to handle multiple connections(both wired and wireless) simultaenously. Internet is accessed through high speed EVDO technology being provided by BSNL.

Our SHNM system hardware has an Intel based system consisting of a Core i3-350M , 2.26 GHz processor, 3 GB RAM ,500 GB hard disk drive, 2 ethernet ports and support for Wireless LAN(802.11b/g/n). Default configuration restricts the commencement of an Internet session from inside the house only. The SHNM features are primarily being provided by an open source packet monitoring tool called Wireshark that has been customized as per our requirement.

Monitoring of packets by Wireshark is being done at the application, transport, network and data-link layer levels. A certain region in the hard disk drive has been reserved as the data storage and housekeeping block wherein all the packets that are being captured are stored. Certain rules have been developed that are applied to this section so that the stored packets are seggregated into the General-Purpose subevent, Interesting subevent and Unsusual subevent block.

The algorithm that has been formulated to be the rule engine is fairly simple and has its base on the application layer and data-link layer only of the TCP/IP model.

As the utility of the SHNM System depends primarily on the recorded data, we investigate the reliability of the Wireshark software to capture the packet events. Experiments were carried out on 3 different hosts in the home to simulate conditions of low, medium and heavy loading conditions. All the tests were carried out for a time span of 1 hour and the percantage of packet loss was calculated. Light loading condition consisted of a music video download and general surfing of the websites. Medium loading condition consisted of 2 torrent downloads(total file size >= 1GB) followed by the normal website surfing. Heavy loading condition consisted of 6 torrent downloads (file size >=5 GB), online video streaming using YouTube, video conferencing for 20 minutes using Skype apart from the normal website surfing.

Table 1 below summarizes the results:

Load Type	**Low**	**Medium**	**Heavy**
Time duration	1 hr.	1 hr.	1 hr.
Packets Captured	46,265	1,36,999	2,51,176
% of Packets Lost	0.032	0.101	0.332

Table 1

.

A graphical plot of the loading condition(i.e packets captured) on the X- axis v/s the percentage of packets lost on the Y- axis has been generated in figure 3 below from the simulated results. The graph is of linear nature which gives us a clear indication that when using Wireshark as a packet monitoring tool the chances of packet loss increases proportionately as the network traffic increases. In fact towards the heavy loading condition the curve becomes much more steeper indicating that the packet losses are even more in the higher end region.

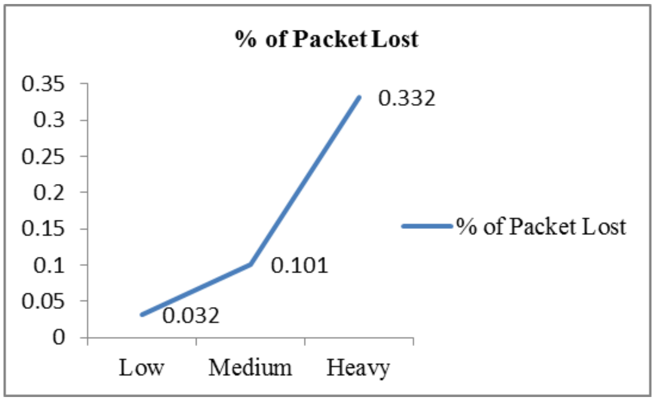

Figure 3

Thus it is evident from the experimental result that for the configuration that we use under heavy loading condition the percentage of packet loss becomes more. Thus, the SHNM System box that we use provides a satisfactory platform for the troubleshooting purpose.

Some systems have been built that enables the home users to visualize the bandwidth been taken up by the different applications and hence control them in a proper manner[12]. Similarly the Eden System[13] uses a customized router for data collection purposes and Home Network Data Recorder(HNDR) Systems [14] tries to figure out the events that happened just prior to a problem occurrence. Similar approach has been attempted for Enterprise Networks also[15].

In the near future we expect to improve the capabilities of our prototype so that it can capture all the network events that have been described earlier. We strongly have an intution that the techniques used by any Intrusion Detection System can be extended to our SHNM system also and so we intend to judiciously mix the functionalities of both. We also have a vision to build up an Extensive Data Search Engine that will have intelligence of its own to detect the causes of home network disruption.

6. CONCLUSION

The paper attempts to provide a solution that is automatic in nature to any problems that can arise in a home network. The entire strength of the proposed solution lies in the capability of the packet monitoring tool. Although Wireshark provides a decent performance for low to medium traffics, but its performance degrades steeply under heavy loading conditions. This is in fact a critical issue today because with the increase in network bandwidth and speeds, multimedia traffic is gaining in more popularity these days, and hence the network traffic is also heavy. Thus an alternative to Wireshark is eminent. The events that are ultimately responsible for network malfunction are logged in a central system as proposed by our architecture. Mixing the SHNM system with the functionalities that are provided by any Intrusion Detection System can be proved to be helpful in increasing the efficiency of our system.

7. REFERENCES

[1] R. Grinter, W.Edwards, M.Newman and N.Ducheneaut. 2005. The work to make a Home Network Work in Proceedings of European Conference on Computer Supported Co-operative Work, Volume 18, page 22, Springer Publication.

[2] Erika Sheehan, Marshini Chetty, Rebecca E. Grinter and Warren Keith Edwards. 2008. More Than Meets the Eye: Transforming the User Experience of Home Network Management in Proceedings of ACM Conference on Designing Interactive Systems (DIS 2008), Cape Town, South Africa.

[3] J.Y.S Marshini Chetty and R.E Grinter. 2007. How Smart Homes Learn: The evolution of the networked home and household in Proceedings of Ubicomp, Innsbruk, Austria.

[4] K. Calvert, W. Edwards and R. Grinter. 2007. Moving towards the Middle: The Case against the End-To-End Argument in Home Networking in Proceedings of 6th ACM Workshop on Hot Topics in Networks (Hotnets-VI), Atlanta, CA.

[5] Erika Sheehan Poole, Marshini Chetty, Tom Morgan, Rebecca E. Grinter and W. Keith. 2009. Computer Help at Home: Methods and Motivations for informal technical support in Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2009), Boston, MA.

[6] B. Agarwal, R. Bhagwan, T. Das, S. Eswaran, V. N. Padmanabhan and G. Voelkar. 2009. Netprints: Diagonising Home Network Misconfigurations using shared Knowledge in Proceedings of 6th USENIX NSDI, Boston, M.A.

[7] M. bin Tariq, M. Motiwala, N. Feamster and M. Ammar. 2009. Detecting Network Neutrality Violations with casual Inference in Proceedings CoNEXT.

[8] S. Hao, N, Syed, N. Feamster, A. Gray and S. Krasser.2009. Detecting Spammers with SNARE: Spatio-temporal Network-Level Automatic Reputation Engine in Proceedings of 18th USENIX Security Symposium, Montreal, Quebec, Canada.

[9] R. Perdisci, W. Lee and N. Feamster. 2010. Behavioural Clustering of HTTP-Based malware in Proceedings of 7th USENIX NSDI, San Jose, CA.

[10] A. Ramachandran, N. Feamster and S. Vempala. 2007. Filtering spam with behavioural blacklisting in proceedings of 14th ACM Conference on Computer and Communications Security, Alexandria, VA.

[11] M.Allman and V. Paxson. 2007. Issues and Etiquette Concerning Use of Shared Measurement Data in Proceedings of ACM Internet Measurement Conference, pages 135-140, San Diego.

[12] M. Chetty, R. Banks, R.Harper, T.Reagan, A.Sellen, C.Gkantsidis, T.Karagiannis and P.Key. 2010. Who's Hogging the Bandwidth? In Proceedings of ACM Human Factors in Computing Systems (CHI) Conference, Atlanta, GA.

[13] J. Yang. 2009. Eden Home Network Management System, Ph.D. dissertation, Georgia Tech.

[14] K. L. Calvert, W. K. Edwards, Nick Feamster, R. E. Grinter, Ye Deng and Xuzi Zhou. 2010. Instrumenting Home Networks in Proceedings of ACM SIGCOMM Workshop on Home Networks, Home Nets '10, pages 55-60, New York, USA.

[15] S.Kandula, R. Mahajan, P. Verkaik, S. Agarwal, J. Padhye and P. Bhal. 2009. Detailed Diagnosis in Enterprise Networks in Proceedings of ACM SIGCOMM, Barcelona, Spain.