ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

Volume No. 11

Issue No. 3

September - December 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

Aims and Scope

Advanced Journal in Wireless and Mobile communication welcomes the original research papers, review papers, experimental investigations, surveys and notes in all areas relating to software engineering and its applications. The following list of sample-topics is by no means to be understood as restricting contributions to the topics mentioned:
•LTE
•4G
•5G
•Ultra wide band communications
•Nnovel mobile applications
•Mobile communications and networking
•Energy-efficient communication networks
•Molecular communications

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

(Volume No. 11, Issue No. 3, September - December 2023)

Contents

SDML based Reusable Web Page Framework for Semantic WEB

Harish Kumar* , Sanjeev Kumar**
*Research Scholar, CMJ Univ. Shillong, Meghalaya
**Supervisor, PIET, Samalkha

ABSTRACT

This paper purposes unique framework for designing reusable web page for Semantic Web. The symbolic web page's design will be stored in unique format of keyword text with the name SBML tag based design. The inference mechanism is facilitated with the help of an inference engine which will search for specific keywords from the design repository. This framework will minimize the overall development effort of designing and developing web pages for semantic web.

Keywords: Agent, Semantic Web, Tag Based Design, Design Repository, Development Efforts

1. INTRODUCTION

This paper addresses the methodology for achieving the web page design reusability of a qualitative web based system and effort minimization by applying the inference on the stored design documents. The pictorial design documents of web pages are stored in a special format in the form of keyword text [SDML tag based design]. The design document storage mechanism will expose the keywords as per design stored. This methodology is having an inference engine. Inference engine search for the keywords and find the match for them in the available design repository. A successful match will help in achieving reusability after checking the quality parameters of the found design module in the result set. SDML notations produce qualitative designs which help in minimizing the efforts of web based system.
Web based development demands not only quick and reliable web page designing but also designing must be reusable. Generally, lot of developer time and efforts are used in developing solutions for difficult, time consuming and complex web based systems. One of the solutions is the web based designs document [2] [3]. Design process takes maximum time and efforts and is never reused in the future. Reusability is achieved up to some level in coding practices like OOPs, Component based developments, Active-X, technology, where a piece of written code is reused after passing through few checks for non discloser of the blueprints of the solution [5].

Design phase is considered to be the most important phase to achieve reusability in web based projects, as it bridges the gap between requirement phase and the development phase. This includes functional and user interaction design. [4] [6]. If a web based design is made reusable, the reusability in the development phases can be achieved because the coding phase is very much driven from the software design. This paper proposes a new approach in the context of the web based design reusability. Reusable web based design methodology is of special concern with the effort minimization, which could be achieved by following this approach. This paper also discusses the notation of the design document storage for reusability. This approach will provide good domain solution in minimum efforts. A good review mechanism can also be imposed on the stored reusable web based design for assigning quality attributes [7] [8][9].

Proposed approach eliminates the need for fresh efforts for web based design every time a solution is required. The web based design document having diagrams, images will be stored in textual format and every design stored will have few keyword and properties [10] [11]. Keyword submission per design facilitates the search against the specified keyword andoutcome of the result having the attribute tag of quality benchmark, like number of times the design is reused. The research also includes one tool, which helps in maintaining the central repository of the different design documents and inference mechanism on the stored design repository.

2 SDML BASED WEB PAGE DESIGN REPRESENTATION FOR SEMANTIC WEB

The reusability of web page design for a software system could be achieved by storing the graphical design documents in the form of text. The graphics-symbols of the design document can be represented in the form of text. Tools are available which allow the user to draw the web page with diagrams. These tools however lack one aspect to store the design elements in the form of structured text as backend.

Our approach is to device some mechanism using which design diagrams for web page can be created and represented in the text format. So that when user creates one web page design and save it, it generates one text file. The approach chosen is to represent the text per design element is as a XML tag. So every design element will have a unique tag as shown in Figure 1.

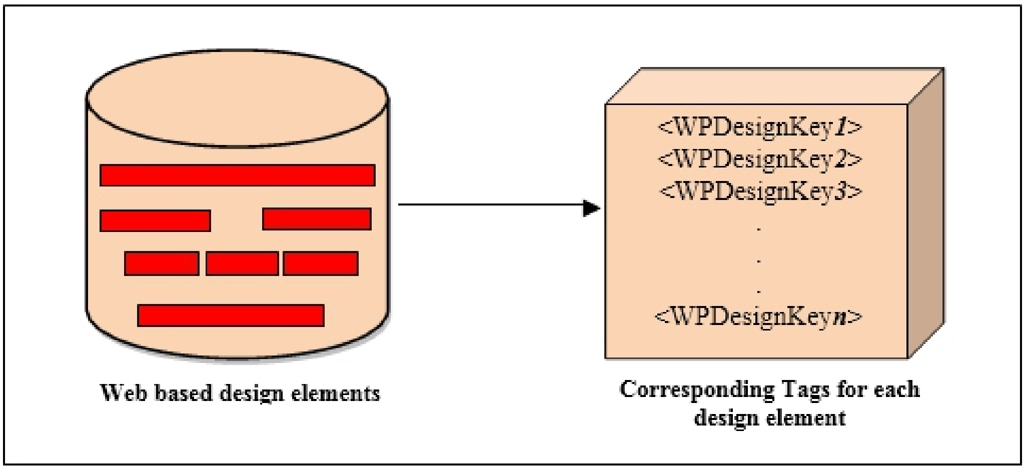

<WPDesignKey1>
<WPDesignKey2>
<WPDesignKey3>
.
.
.
<WPDesignKeyn>
Web based design elements
Corresponding Tags for each design element

Figure 1: Every web page design element is having web page design element tag associated with it.

Initially the process start with making a new web page design document, which is XML, based. The system to create the web page design is having the collection of web page elements. All finite design elements have assigned names. User has to select and place these design elements while creating design document. When one web page design gets completed, there will be one complete XML document associated with it. These web page design repository will be a collection of associated XML document per design as shown in Figure 2.

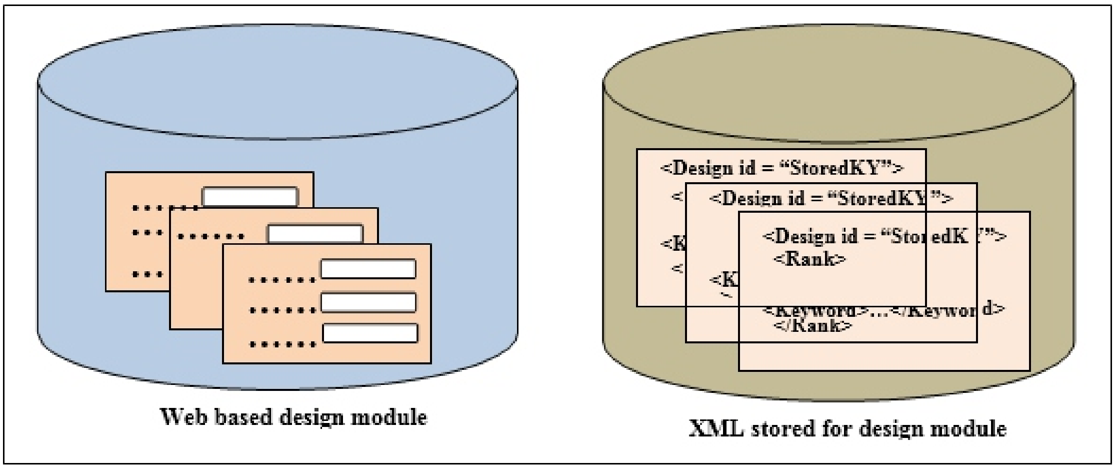


Figure 2: Each design module is having associated SDML document

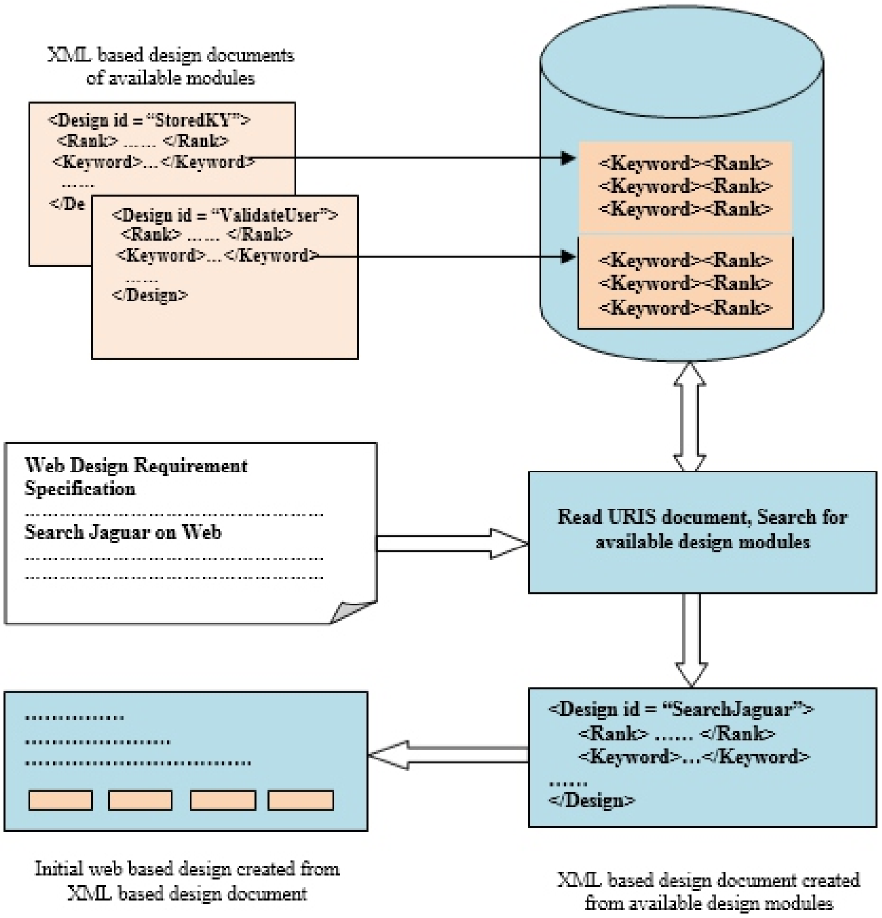
There will be a repository of designs after following this approach and every design is well defined in terms of XML tags. The text format of storing the design is having the predefined tags. Text format will be stored in XML notations. This is termed as Semantic Design Markup Language and is having the tags for all knows design elements. When user picks one design element, its respective tag will be placed in its corresponding text file. When web page design complete for some scenario by following this approach, system will be having a complete representation in textual format in the form of tags.

The XML text file having the details of design figures is the basis of our research. The approach has many benefits. When pictorial representations are saved in text form, lots of possibilities are there which increase the efficiency of overall development process [12] [13]. Reusability of design search within the available web page design, automatic generation of design skeleton on the basis of requirement document and available design text keywords, auto generation of test case scenarios.

Along with the design element tags, the XML-SDML file is having the information with the help of special tags (like <keywords>), which is important and is a key for further reusability criteria implementation and page rank number, which is used by Personal Agent and Service Agent for agent based web page semantic search [1]. This additional information is the list of keywords that designer wants to assign to his design. Each web page design is having one name, keywords and some attributes.
Name identifies the design module, keywords are the handles for reusability, and attributes are factors, which design document gain after reusability. Agents review the web page designand assign ranks to each keyword in a web page. A high rank number by agent make web page design a good candidate for reusability for particular type of user.

When some user wants to search the new web page based upon some keyword, he has to submit the keywords to be search to the Personal Agent. The keywords are analyzed and some keywords are evaluated by Personal Agent in terms of ranking. Next step is that agent looks into the available keywords of design module repository for the specific keyword. The design repository will be stored for each design element in a centralized database of the Personal Agent. The design stored is of the atomic nature by representation of text format.

sign>Each elementary design element will be having one name and some associated keywords. These keywords will be reflected in the centralized repository.



sign>Each elementary design element will be having one name and some associated keywords. These keywords will be reflected in the centralized repository.

Figure 3: Mechanism for web page design reusabilityIn software development life cycle, when analysis phase is completed and the requirements are defined, next stage is to move to design process. The existing design repository will help out in reusing the design elements. Above figure shows the mechanism for web page design reusability. After following the approach for creating XML based web page design documents (SDML), there will be a database of XML sheets for each design module. Each design module is having the name and keywords associated with it.

< !ELEMENT name *>
< !ELEMENT keywords *>

Inference will be preformed on the centralized design repository against the keywords from the Personal Agent. This will be a type of look-in search process in the design repository keywords of elementary design. When search gets completed, it will generate a minimum web page design document having the maximum reusability of existing modules. This SDML document is arranged in order to get the maximum requirement fulfillment for required web page design.

Also, the result of the inference on stored design repository will be having the elementary design modules having attributes also. These attributes specify the design reusability factor for a module

(DRF). More the reusability factor of a module indicates that module is strong candidate for reusability in new design. Reusing a web page design module will increase the reusability count factor by one.

Design storage and retrieval

A.) Create SDML based web page design and generate design repository per design module. Figure4 is the logical representation while creation of new design. If user creates the new design and it is driven from some existing design element Dg..n, it will increment the design reusable factor DRF for Dg..n by one. This increment in DRF make makes design Dg..n a stronger candidate for further reusability

B.) Retrieve SDML based design repository for reusability and create initial proposed design layout. The following flow chart (Fig 4) shows how the DRF (Design Reusable Factor) helps in reusing the existing web page design. First the search for the keywords in existing design will be performed. The outcome then will be sorted in descending order on the bases in DRF. The top value of result outcome shows that first one in the search is the best candidate for reusability.

3. EXPERIMENT SETUP

For the experimental validation of the proposed approach of web page design reusability and effort minimization, five keywords have been considered. These keywords are having maximum of six different sub keywords. Web page design requirement for these modules have been studied and one end user is considered for the experiment to which the finished design will be given for review. From requirement discussion to first draft, we record the time spend for each keyword. We also record the time consumed by the web page design architect. When this gets finished, we need to discuss it with the end user. Time record for the end user involvement was also recorded. We include the end user in the design phase for layout, look and feel type observation. We consider this as design prototype.

4. RESULT AND OBSERVATIONS

Table 1 is the record of the efforts made by the web page design architect and end user for verification of the initial draft. This is the observation of the projects using conventional system and we will compare it with efforts consumed using our approach in next section with Table 2.

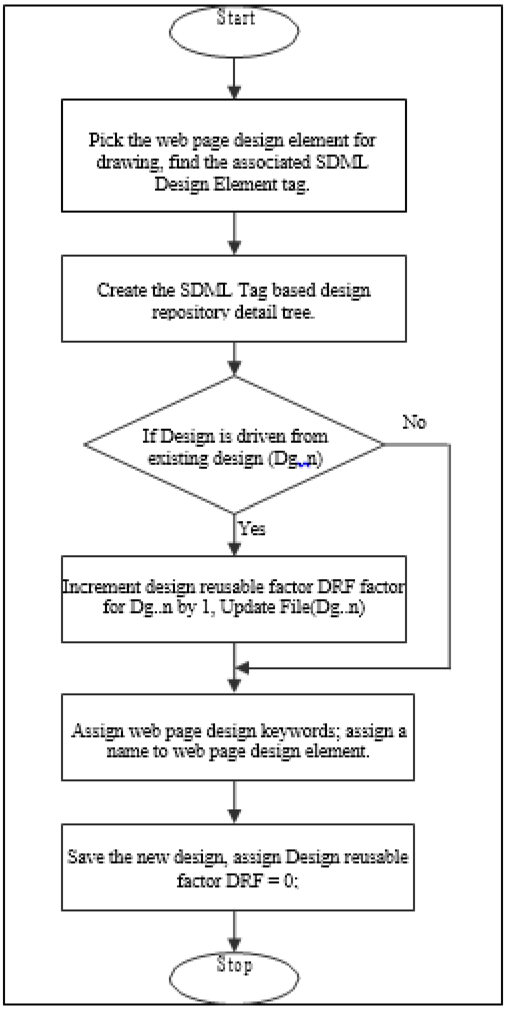

Start
Pick the web page design element for drawing, find the associated SDML Design Element tag.
Create the SDML Tag based design repository detail tree.
If Design is driven from existing design (Dg..n)
No
Yes
Increment design reusable factor DRF factor for Dg..n by 1, Update File(Dg..n)
Assign web page design keywords; assign a name to web page design element.
Save the new design, assign Design reusable factor DRF = 0;
Stop

Figure 4: Create SDML based web page design

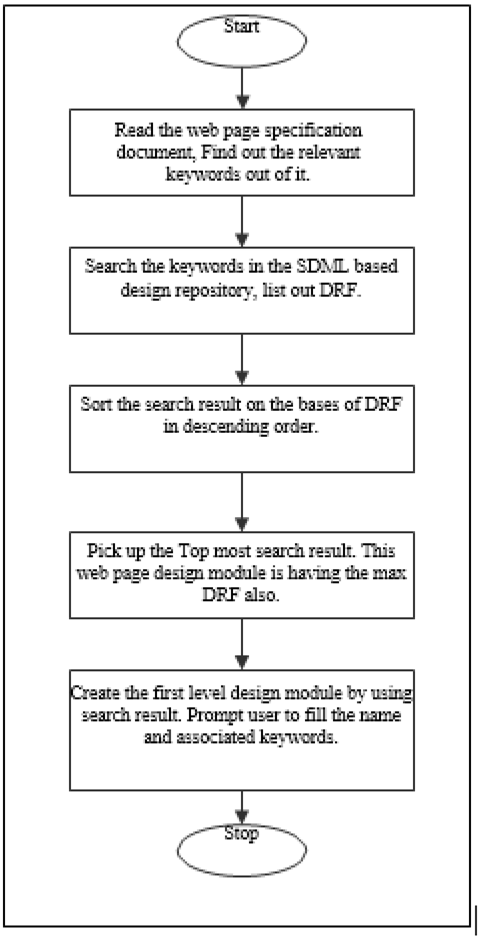
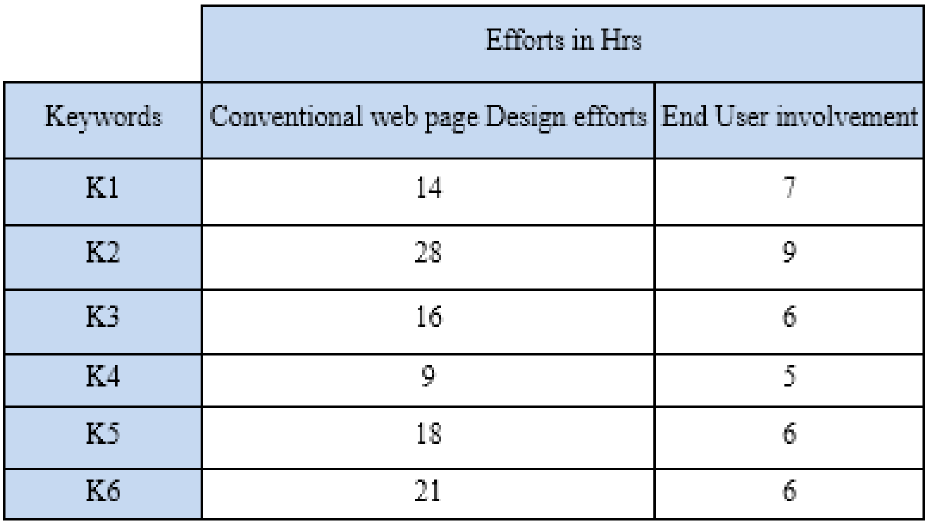

Start
Read the web page specification document, Find out the relevant keywords out of it.
Search the keywords in the SDML based design repository, list out DRF.
Sort the search result on the bases of DRF in descending order.
Pick up the Top most search result. This web page design module is having the max DRF also.
Create the first level design module by using search result. Prompt user to fill the name and associated keywords.
Stop

Figure 5: Retrieve SDML based design repository for web page design reusability



	Efforts in Hrs	
Keywords	Conventional web page Design efforts	End User involvement
K1	14	7
K2	28	9
K3	16	6
K4	9	5
K5	18	6
K6	21	6

Table 1: Efforts (in Hrs) in web page design using conventional design methods

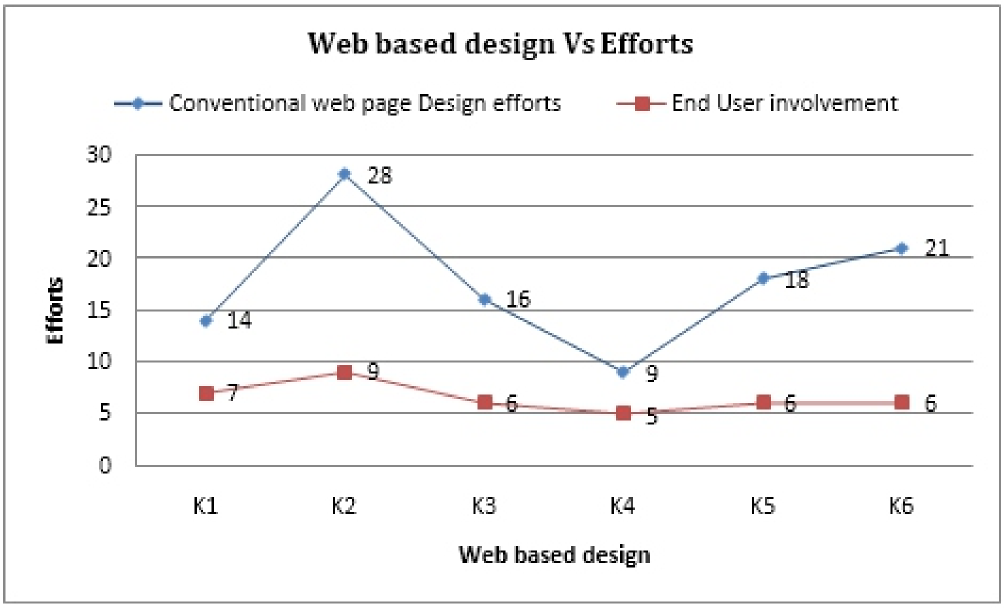


Figure 6: Efforts (in Hrs) in web page design using conventional design methods (Source: Table 1)

The graph (Figure 6) represents that for a project of 4 modules, minimum time for design is 13 hrs where as maximum could be 29 hrs for a project of 4 modules. This variation shows that module count is immaterial but the important is nature of project. This observation when compared with the SDML based approach will shows very interesting results.

For our experiment with SDML based web page design, we are having 10 designs in the SDML storage and these are having 50% resemblance with the domain of the requirement. These design documents are having the keywords, which could be used during the search process. The SDML based design experiment for the reusability of existing design requires the framing of the requirement specification in some special format. So, we have made the requirement specification document. This is having the keyword-based text instead of the plain English based scenario discussions. Same projects with special formatting of the requirement specification are submitted to SDML inference engine.

This takes very less time in identifying the candidate from available stored design and displays the results. The time taken in framing the requirement and getting the first level design from existing designs is shown in the following table (Table 2). Its approximately 1hr because this is not simply selection process, user have to spend some time (in few min) to identify which one is appropriate on the bases of some ranks, like reusability factor. Observations in Table 2 are showing the improvement in the efforts consumed. The only efforts consumed are in the framing of the requirement in the special format. The agile client efforts, which can be a part of team also need to spend small time as compared to time spend in Table1 by the user [14][15]. We propose the involvement of the user in the design process with our mechanism. User interactions could be of the type of selecting one design layout out of available design layout produced by the system.

	Efforts in Hrs			
Keywords	Efforts in Framing Requirements	Effort in generating first level design	Agile client efforts	Total efforts in automation
K1	6	1	1	8
K2	9	1	2	12
K3	8	1	2	11
K4	5	1	1	7
K5	4	1	3	8
K6	8	1	2	11

Table 2: Efforts (in Hrs) in web page design using SDML based web page design methods

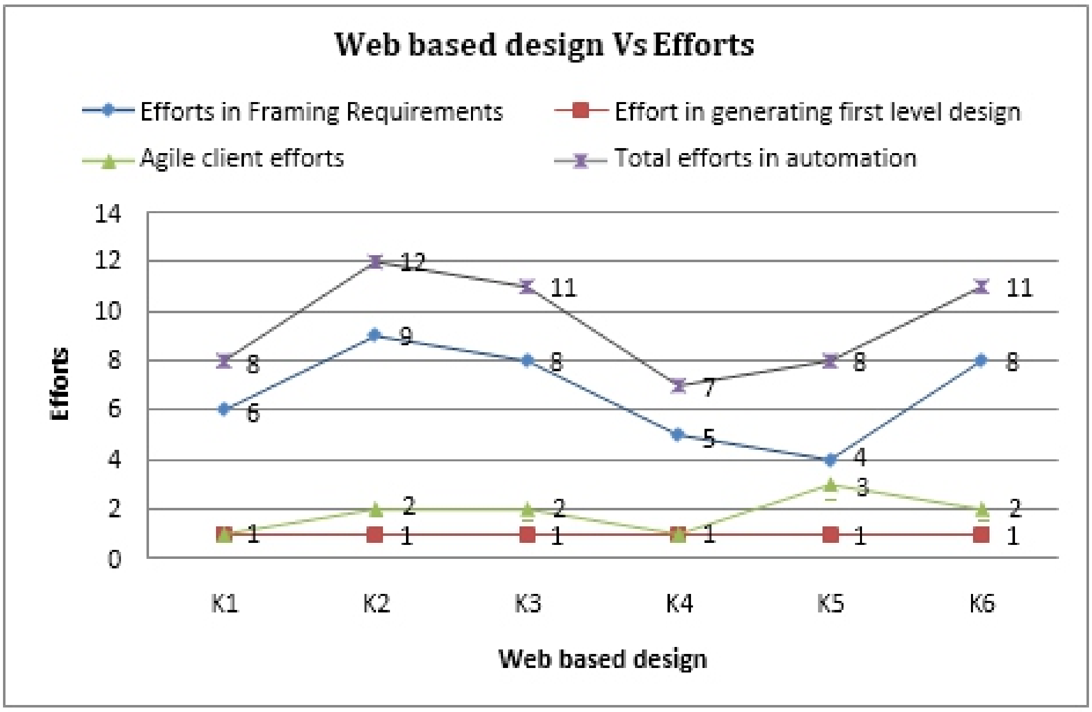


Figure 7: Efforts (in Hrs) in web page design using conventional design methods (Source: Table2)

The total time consumed in the finalization which is summation of time consumed in framing requirement, design generation by system and client time to select. We represent this as TED, i.e. total effort required for SDML based design.

$$TED = \sum_{i\in SP} RFi \oplus DGi \oplus ACEi$$

RF is the efforts required for requirement framing for software project SP, DG is efforts in design generation and ACE is the agile client efforts. Figure 6 shows the graphical representation for the same.

As an observation from Figure 7 we can see the total efforts consumed in the proposed design are less than that of conventional system which is showing the effort minimization after using the SDML based design approach and then applying the DNSIM (Design notation storage and inference mechanism) for reusing the same for achieving the qualitative designs.

Keywords	Total efforts in SDML based approach	Total efforts in conventional web page design.
K1	8	19
K2	12	37
K3	11	24
K4	7	12
K5	8	26
K6	11	27

Table 3: Total Efforts comparison in using two approaches

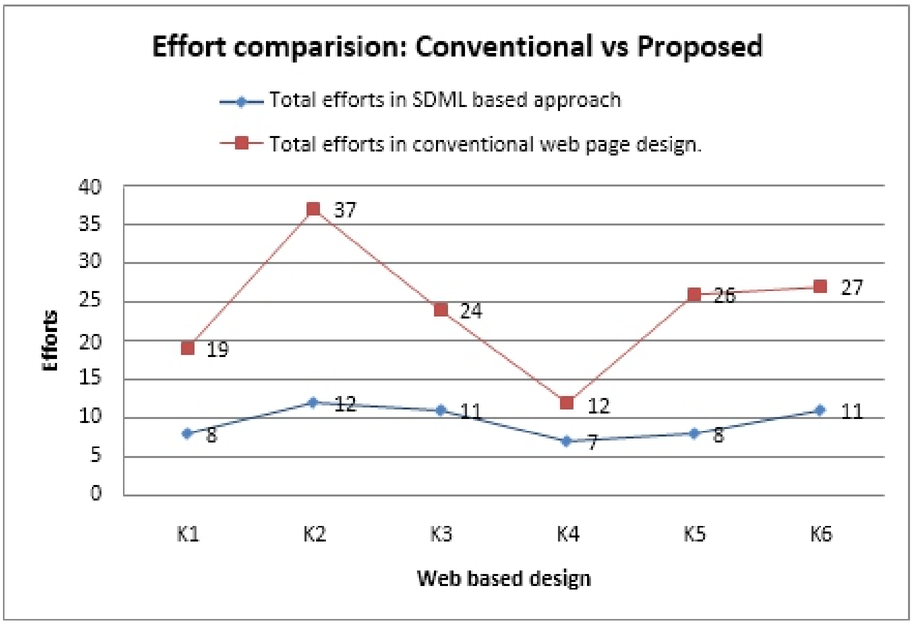


Figure 8: Total Efforts comparison: SDML based approach and conventional approach (Source: Table3)

Graphs (Figure 8) shows the comparison and figures in the total effort minimization. SDML based design approach uses requires the less effort, as compared to other methods. SDML based approach produces qualitative design, which helps in minimizing overall efforts in software development life cycle. The end user involvement and efforts for feedback are comparatively less in case of the SDML based approach. For same projects taken in our experiment, we found that there is a big difference in the end user involvement. As for project1 having 4 modules, the efforts consumed by the agile client for feedback are 6hrs for conventional approach where as its only 1hr required for the SDML based user interface design. This also represents that it's a qualitative design approach towards effort minimization and making SDLC less complex.

Keywords	End User involvement. (Conventional)	Agile client efforts
K1	6	1
K2	8	2
K3	7	2
K4	4	1
K5	7	3
K6	7	2

Table 4: User involvement efforts comparison in using two approaches.

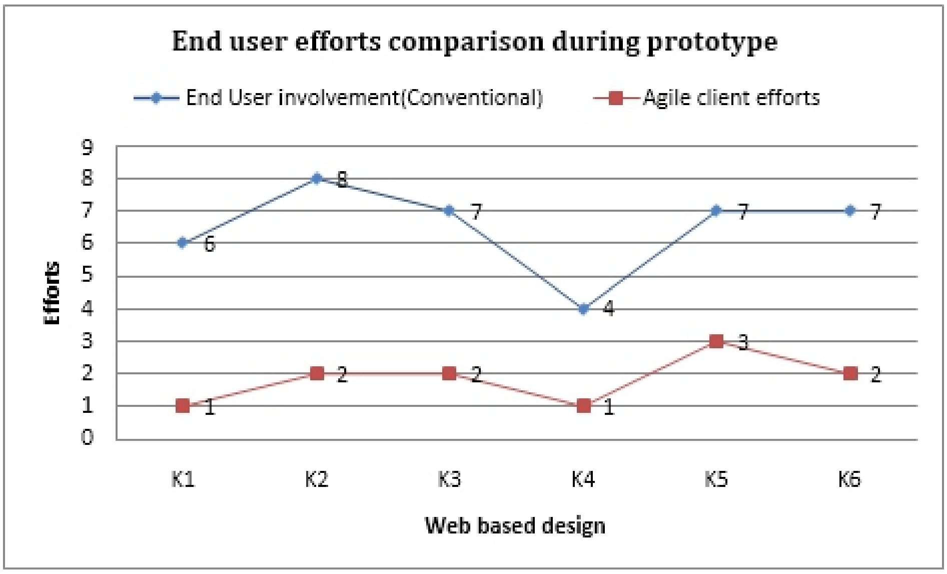


Figure 9: Total Efforts comparison: SDML based approach and conventional approach (Source: Table3)

5 CONCLUSION

SDML based designs representation is a new approach for storing the design elements in the form of specially design SDML-XML tags. These are plain text files, so we can write programs to manipulate and analyze these files for further enhancement.

To simulate the effort minimization, we carry out above-mentioned experiment. It shows that the there is tremendous decrease in the user involvement. We carry out our experiment on five different projects having different number of modules. Table 1 is showing the efforts in man hrs and end user involvement using the conventional, approaches of software design engineering. The graph in the Figure6 depicts that there is big involvement of the end user in the design phase (we consider agile methodology where customer is a member of development team) as for project2 29 hr efforts are from designer team and end user spend 8 hrs.

Table 2 shows the overall efforts for creating the first level design using SDML based approach. The total efforts in automation are less than that of the manual and conventional system. There is a significant minimization in the efforts of the agile client involvement as depicted from the Figure 7 and Table 2.

Figure 8 shows the comparison between the total efforts of SDML based design and conventional design. In SDML based design, there is only on activity, which consumes time and that is the framing of the requirement specification document. This contains finding out the important keywords from the requirement specification document and using them later in the search process SDML based parsing.

Figure 9 compares the involvement of the end user in the same projects using the two different approaches. It clearly shows that agile client involvement is reduced significantly after following the SDML based approach.

The web page design reusability leads to faster development of the application especially in the area where the web page is of prime importance. Big time and efforts, which are consumed in developing the core web page design functionality, could be minimized. The user involvement in the design phase and efforts could be minimized in the design process. This is because the design elements are stored in the textual format and we can apply several kinds of search algorithms for finding the best solution for the problem. Further, design storage in specified format makes the system scalable and maintainable. The approach of the reusability of software design is novel. Work presented in this paper is an initiative towards using SDML based web page design representation for reusability. The experiment carried on five keywords for effort minimization using web page design reusability is showing interesting and valuable observation of the concept.

6 BIBLIOGRAPHY

[1] Franklin, S., Graesser, A.,” Is it an agent, or just a program?” Proceedings Third International Workshop on Agent Theories, Architectures and Languages, Budapest, Hungary, 193-206. 1996

[2] Markopoulos P., Wilson S., Johnson and P., "Representation and use of task knowledge in a user interface design environment", Computers and Digital Techniques, IEEE Proceedings, Volume 141, Issue 2, pp: 79-84, 1994.

[3] Yam Li [2009], "Intelligent User Interface Design Based on Agent Technology", software Engineering, WCSE '09. WRI World Congress, Volume 1, 19-21 May 2009, pp: 226-229. 2009.

[4] Tesarik J., Dolezal L. and Kollmann C., "User interface design practices in simple single page web applications", Applications of Digital Information and Web Technologies, ICADIWT 2008. First International Conference on the 4-6 Aug. 2008, pp: 223-228. [2008]

[5] Hood Meier Halo; Afar, A., "Tracing user interface design pre-requirement to generate interface design specification", Electrical Engineering and Informatics, ICEEI 'Aug. 2009, pp: 287-292, 2009.

[6] Doane S.M. and Lemke A.C., "Using cognitive simulation to develop user interface design principles", System Sciences, Proceedings of the Twenty-Third Annual Hawaii International Conference on Volume ii, pp: 547-554, 1990.

[7] Bajwa I.S. and Chaudhary M.A., "A Language Engineering System for Graphical User Interface Design (LESGUID): A Rule based Approach", Information and Communication Technologies, 2006. ICTTA '06. 2nd Volume 2, pp: 3582 – 3586, 2006.

[8] Ping Zhang; Small, R.V. von Dran, G.M. Barcellos S., "Websites that satisfy users: a theoretical framework for Web user interface design and evaluation", System Sciences, HICSS-32, Proceedings of the 32nd Annual Hawaii International Conference on Volume Track2, pp: 8, Jan. 1999.

[9] Vila J., Beccue B., Furness G., "User interface design for virtual reality: a research tool for tracking navigation", System Sciences, Proceedings of the Thirty-First Hawaii International Conference on Volume 6, 6-9 Jan. 1998, pp: 464-472, 1998.

[10] Maskers J.; Layton K.; Coning K., "Shortening user interface design iterations through real-time visualization of design actions on the target device", Visual Languages and Human-Centric Computing, VL/HCC 2009, IEEE Symposium, pp: 132-135, 2009.

[11] Sunhat V.S., Sukaviriya and Ramachandra, T., "Using User Interface Design to Enhance Service Identification of Web Services", ICWS '08. IEEE International Conference on 23-26 Sept. 2008, pp: 78 – 87, 2008,

[12] Lindgaard G., “Designing CSCW tools to support cooperative research", Computer Human Interaction Conference, Proceedings. Australasian, 30 Nov.-4 Dec. 1998, pp: 61-62, 1998,

[13] Balasubramanian V., Turoff M., "A systematic approach to user interface design for hypertext systems", System Sciences, Proceedings of the twenty-Eighth Hawaii International Conference on Volume 3, 3-6, pp: 241–250, Jan. 1995.

[14] Stary C., "User interface design: the WHO, the WHAT, and the HOW revisited", Computer Software and Applications Conference, COMPSAC 95. Proceedings, Nineteenth Annual International 9-11 Aug. 1995, pp: 178-183, 1995.

[15] Quiroz J.; Shankar, A.; Dascalu, S.M.; Louis, S.J.;, "Software Environment for Research on Evolving User Interface Designs", Software Engineering Advances, 2007. ICSEA 2007. International Conference on 25-31 Aug. 2007, pp: 84-84, 2007.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) For Network Security: A Critical Analysis

Sandeep Singh*
*Student,
M. Tech. (I.T.),

ABSTRACT

This paper analyzes and criticizes the ways of functioning of IDS and IPS. Understanding the similarity of characteristics of IDS and IPS may be useful in making decisions regarding their use in Organizational Computer Network. To deploy IDS or IPS we need to understand the types of IDS and IPS and the way they operate when an attack is launched. Intrusion Prevention Systems can be Host based (HIPS) and Network Based (NIPS). Finally, knowledge of Signature and Signature alarms will make the administrative tasks easier.

Keywords: Intrusion detection system, IDS, Intrusion prevention system, IPS, Signature, signature micro-engines, signature alarms, Host based IPS, HIPS, Network based IPS, NIPS, Network Security

Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions form an integral part of a robust network defense solution. Maintaining secure network services is a key requirement of a profitable IP-based business.

INTRODUCTION TO IDS AND IPS:-

IDS and IPS work together to provide a network security solution. An IDS captures packets in real time, processes them and can respond to threats, but works on copies of data traffic to detect suspicious activity by using signatures. This is called promiscuous mode. In the process of detecting malicious traffic, an IDS allows some malicious traffic to pass before the IDS can respond to protect the network. An IDS analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating on a copy of the traffic is that the IDS does not affect the packet flow of the forwarded traffic. The disadvantage of operating on a copy of the traffic is that the IDS cannot stop malicious traffic from single- packet attacks from reaching the target system before the IDS can apply a response to stop the attack. An IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack.

An IPS works inline in the data stream to provide protection from malicious attacks in real time. This is called inline mode. Unlike an IDS, an IPS does not allow packets to enter the trusted side of the network. An IPS monitors traffic at Layer 3 and Layer 4 to ensure that their headers, states and so on are those specified in the protocol suite. However, the IPS sensor analyzes at Layer 2 to Layer 7 the payload of the packets for more sophisticated embedded attacks that might include malicious data. This deeper analysis lets the IPS identify, stop and block attacks that would normally pass through a traditional firewall device. When a packet comes in through an interface on an IPS, that packet is not sent to the outbound or trusted interface until the packet has been determined to be clean. An IPS builds upon previous IDS technology.

IDS AND IPS TECHNOLOGIES SHARE SEVERAL CHARACTERISTICS:-

- **IDS and IPS technologies are deployed as sensors. An IDS or an IPS sensor can be any of the following devices:**
  - A router configured with IPS software
  - An appliance specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance, switch or router

- **IDS and IPS technologies typically monitor for malicious activities in two spots:**
  - Malicious activity is monitored at the network to detect attacks against a network, including attacks against hosts and devices, using network IDS and network IPS.
  - Malicious activity is monitored on a host to detect attacks that are launched from or on target machines, using host intrusion prevention system (HIPS). Host based attacks are detected by reading security event logs, checking for changes to critical system files, and checking system registries for malicious entries.
  - IDS and IPS technologies generally use signatures to detect patterns of misuse in network traffic. A signature is a set of rules that an IDS or IPS uses to detect typical intrusive activity. Signatures are usually chosen from a broad cross section of intrusion detection signatures and can detect severe breaches of security, common network attacks and information gathering.

- **IDS and IPS technologies look for the following general patterns of misuse:**

- **Atomic pattern:** In an atomic pattern, an attempt is made to access a specific port on a specific host, for any malicious content contained in a single packet. An IDS is particularly vulnerable to an atomic attack because until it finds the attack, malicious single packets are being allowed into the network. An IPS prevents these packets from entering at all.

- **Composite pattern:** A composite pattern is a sequence of operations distributed across multiple hosts over an arbitrary period of time.

Steps that occur when an attack is launched in an environment monitored by an IDS: Step 1. An attack is launched on a network that has a sensor deployed in IDS mode.

Step 2. The switch sends copies of all packets to the IDS sensor (Configured in promiscuous mode) to analyze the packets. At the same time, the target machine experiences the malicious attack.

Step 3. The IDS sensor, using a signature, matches the malicious traffic to the signature.

Step 4. The IDS sensor, sends the switch a command to deny access to the malicious traffic.

Step 5. The IDS sends an alarm to a management console for logging and other management purposes.

Steps that occur when an attack is launched in an environment monitored by an IPS:

Step 1. An attack is launched on a network that has a sensor deployed in IPS mode (configured in inline mode)

Step 2. The IPS sensor analyzes the packets as soon as they come into the IPS sensor interface. The IPS sensor, using signatures, matches the malicious traffic to the signature and the attack is stopped immediately. Traffic in violation of policy can be dropped by an IPS sensor.

Step 3. The IPS sensor can send an alarm to a management console for logging and other management purposes.

TYPES OF IDS AND IPS SYSTEMS:-

1. Signature-Based IDS/IPS Systems:

A signature-based IDS or IPS sensor looks for specific, predefined patterns (signatures) in network traffic. It compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found. The signature can be based on a single packet or a sequence of packets. New attacks that do not match a signature do not result in detection. For this reason, the signature database needs to be constantly updated.

Signature-based pattern matching is an approach that is rigid but simple to employ. In most cases, the pattern is matched against only if the suspect packet is associated with a particular service or, more precisely, destined to and from a particular port. This matching technique helps to lessen the amount of inspection done on every packet. However, it makes it more difficult for systems to deal with protocols that do not reside on well-defined ports, such as Trojan horses and their associated traffic, which can move at will.

At the initial stage of incorporating signature-based IDS or IPS, before the signatures are tuned, there can be many false positives (traffic generating alert which is not threat for the network). After the system is tuned and adjusted to specific network parameters, there will be fewer false positives than with the policy-based approach.

2. Policy-Based IDS/IPS Systems:

In policy-based systems, the IDS or IPS sensor is preconfigured based on the network security policy. The policies used in a policy-based IDS or IPS must be created. Any traffic detected outside the policy will generate an alarm or will be dropped. Creating a security policy requires detailed knowledge of the network traffic and is a time-consuming task.

Policy-based signatures use an algorithm to determine whether an alarm should be fired. Often, policy-based signature algorithms are statistical evaluations of the traffic flow. For example, in a policy-based signature used to detect a port sweep, the algorithm issues an alarm when the threshold number of unique ports is scanned on a particular machine. Policy- based signature algorithms can be designed to analyze only specific types of packets (for example, SYN packets, where the SYN bit is turned on during the handshaking process at eh beginning of the session).

The policy itself may require tuning. For example, you might have to adjust the threshold level of certain types of traffic so that the policy conforms to the utilization patterns on the network that it is monitoring. Policies can be used to look for very complex relationships.

3. Anomaly-Based IDS/IPS Systems:

Anomaly-Based or profile-based signatures typically look for network traffic that deviates from what is seen "normally". The biggest issue with this methodology is that you first must define what normal is. If during the learning phase your network is the victim of an attack and you fail to identify it, the anomaly-based IPS systems will interpret that malicious traffic as normal, and no alarm will be triggered next time this same attack takes place. Some systems have hard-coded definitions of normal traffic patterns and, in this case, could be considered heuristic-based systems.

Other systems are built to learn normal traffic behavior; however, the challenge with these systems is eliminating the possibility of improperly classifying abnormal behavior as normal. Also, if the traffic pattern being learned is assumed normal, the system must contend with how to differentiate between allowable deviations, and those deviations that are not allowed or that represent attack-based traffic. Normal network traffic can be difficult to define.

The technique used by anomaly-based IDS/IPS systems is also referred as network behavior analysis or heuristics analysis.

4. Honeypot-Based IDS/IPS Systems:

Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns. You can use this analysis to tune your sensor signatures to detect new types of malicious network traffic.

Honeypot systems are used in production environments, typically by large organizations that come across as interesting targets for hackers, such as financial enterprises, governmental agencies, and so on. Also, antivirus and other security vendors tend to use them for research.

IPS ACTIONS:-

When an IPS sensor detects malicious activity, it can choose from any or all the following actions:

- **Deny traffic inline:** This action terminates the current packet and future packets from this attacker address for a specified period of time. The sensor maintains a list of the attackers currently being by the system. You can remove entries from the list or wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset, and attacker A remains on the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.

- **Deny connection inline:** This action terminates the current packet and future packets on this TCP flow. This is also referred to as deny flow.

- **Deny packet inline:** This action terminates the packet.

- **Log 'attacker packets':** This action starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the event store, which is local to the IOS router, even if the produce-alert action is not selected.

- **Log 'pair packets':** This action starts IP logging on packets that contain the attacker and victim address pair. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.

- **Produce alert:** This action writes the event to the event store as an alert.

- **Produce verbose alert:** This action includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.

- **Request block connection:** This action sends a request to a blocking device to block this connection.

- **Request block host:** This action sends a request to the blocking device to block this attacker host.

- **Request SNMP trap:** This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. This action causes an alert to be written to the event store, even if produce-alert action is not selected.

- **Reset TCP connection:** This action sends TCP resets to hijack and terminate the TCP flow.

EVENT MONITORING AND MANAGEMENT:-

Event monitoring and management can be divided into the following two needs:

- The need for real-time monitoring and management
- The need to perform analysis based on archived information (reporting)

These functions can be handled by a single server, or the functions can be placed on separate servers to scale the deployment. The number of sensors that should forward alarms to a single IPS management console is a function of the aggregate number of alarms per second that are generated by those sensors (25 or fewer; where a mixture of default and tuned signatures are used).

Host and Network IPS:-

IPS technology can be network based and host based. There are advantages and limitations of both but in many cases, they are thought to be complementary.

Host-Based IPS (HIPS) :

HIPS audits host log files, host file systems and resources. A significant advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on that specific host. HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls and application firewalls in one package.

HIPS operates by detecting attacks that occur on a host on which it is installed. It works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests and analyzing local log files for after-the fact suspicious activity.

Precisely, HIPS functions according to the following steps:

Step 1. An application calls for system resources

Step 2. HIPS checks the call against the policy

Step 3. Requests are allowed or denied

HIPS uses rules that are based on a combination of known attack characteristics and a detailed knowledge of the operating system and specific applications running on the host. These rules enable it to determine abnormal or out-of-band activity.

Network-Based IPS (NIPS) :

Network IPS involves the deployment of monitoring devices, or sensors, throughout the network to capture and analyze the traffic. Sensors detect malicious and unauthorized activity in real time and can take action when required. Sensors are deployed at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the attack target. Network IPS sensors are usually tuned for intrusion prevention analysis. The underlying operating system of the platform on which the IPS software is mounted is stripped of unnecessary network services, and essential services are secured (i.e. hardened). The hardware includes the following components:

- **Network Interface Card (NIC):** Network IPS must be able to connect to any network (Ethernet, Fast Ethernet, Gigabit Ethernet)

- **Processor:** Intrusion prevention requires CPU power to perform intrusion detection analysis and pattern matching

- **Memory:** Intrusion detection analysis is memory intensive. Memory directly affects the capability of a network IPS to efficiently and accurately detect an attack.

Network IPS gives security managers real-time security insight into their networks regardless of network growth. Additional hosts can be added to protected networks without needing more sensors. When new networks are added, additional sensors are easy to deploy. Additional sensors are required only when their rated traffic capacity is exceeded, when their performance does not meet current needs, or when a revision in security policy or network design requires additional sensors to help enforce security boundaries.

Signatures and Signature Engines :-

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks.

As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature, and an IDS or IPS sensor examines the data flow using many different signatures.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. False positives can be minimized by tuning the sensors. Signatures can be tuned by adjusting many signature parameters.

Examining Signature Micro-Engines:

A signature micro-engine is a component of an IDS and IPS sensor that supports a group of signatures that are in a common category. Each engine is customized for the protocol and fields that it is designed to inspect and defines a set of legal parameters that have allowable ranges or sets of values. The signature micro-engines look for malicious activity in a specific protocol. Signatures can be defined for any of the supported signature micro-engines using the parameters offered by the supporting micro-engine. Packets are scanned by the micro- engines that understand the protocols contained in the packet.

When IDS (promiscuous mode) or IPS (inline mode) is enabled, a signature micro-engine is loaded (or built) on to the router. When a signature micro-engine, the router may need to compile the regular expression found in a signature. Compiling a regular expression requires more memory that the final storage of the regular expression.

A regular expression is a systematic way to specify a search for a pattern in a series of bytes. For example, a regular expression used to prevent data containing .exe or .com or .bat from crossing the firewall could look like this:

“.*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])”

Signature Alarms :

The capability of IDS and IPS sensors to accurately detect an attack or a policy violation and generate an alarm is critical to the functionality of the sensors. Attacks can generate the following types of alarms:

- **False positive:** A false positive is an alarm triggered by normal traffic or a benign action. For example a wrong password entered mistakenly by a genuine user may result in false positive. The sensor cannot differentiate between a rogue user and a mistaken user.

- **False negative:** A false negative occurs when a signature is not fired when offending traffic is detected. A false negative should be considered a software bug only if the IDS and IPS have a signature that has been designed to detect the offending traffic.

- **True positive:** A true positive occurs when an IDS and IPS signature is correctly fired, and an alarm is generated, when offending traffic is detected.

- **True negative:** A true negative occurs when a signature is not fired when non- offending traffic is captured and analyzed. In other words, the sensor does not fire an alarm when it captures and analyzes “normal” network traffic.

An Insight of SSL Security Attacks

Zubair Jeelani* Owais*
*Department of Computer Science, Islamic University of Science and Technology, J&K, India.

ABSTRACT

Secure Sockets Layer (SSL), is a cryptographic protocol that provide communication security over the Internet. SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity. SSL secures web services such as banking, online purchases, email and remote access. SSL has been targeted with attacks from the time it was created. Most of these attacks exploit the vulnerabilities present in the services SSL use, such as digital certificates and the web browsers. Attacks on SSL itself have been successful, at least in the context of research, attacks on the services that SSL uses have been successfully exploited in an actual commercial setting; the fact that makes these kinds of attacks extremely dangerous. In this paper, we briefly explain the various attacks like SSL sniffing, MD5 collide certificate, SSL striping, SSL Null prefix, online certificate status protocol (OCSP),change cipher spec- dropping, KeyExchangeAlgorithm-spoofing, and version rollback attacks. Since most of the discussed attacks target browsers and the way they manage certificates, an evaluation on the rate of success of the SSL attacks when various browsers are used is also presented. We also discuss the origin and the conditions for the attacks to happen successfully. We further discuss in some detail the two very recent attacks BEAST (Browser Exploit Against SSL/TLS) and CRIME (Compression Ratio Info-leak Made Easy).

Keywords: Secure sockets layer; digital certificates; SSL attacks

1. INTRODUCTION

The recent explosive growth of the Internet and the World Wide Web has brought with it a need to securely protect sensitive information sent over this open network, such as credit card information, usernames, and passwords. Secure Sockets Layer or SSL is a protocol responsible for transmitting this sensitive information in a secure manner by achieving data confidentiality, integrity and authentication in Web transactions.

SSL through a cryptographic system uses two keys to encrypt dat‒a a public key known to everyone and a private or secret key known only to the recipient of the message. SSL works between the OSI Application and Transport layers to provide for the client and server applicable connection oriented mechanisms for secure communication channel.

Even with the presence of some attacks that are able to extract various transmitted secure credentials, SSL has been increasingly used since its introduction. Several attacks have been successfully conducted on the SSL. These attacks can either exploit the implementation of the protocol itself or may exploit the vulnerabilities in the services SSL uses. In this paper, Section 1 provides a brief overview of the SSL protocol. Section 2 explores several attacks on the SSL and Section 3 concludes the paper by providing a high-level view of the SSL protocols strengths and weaknesses.

2. OVERVIEW OF SSL

SSL has two distinct entities, server and client. The client is the entity that initiates the transaction, whereas the server is the entity that responds to the client and negotiates which cipher suites are used for encryption. In SSL, the Web browser is the client and the Web- Server is the Server.

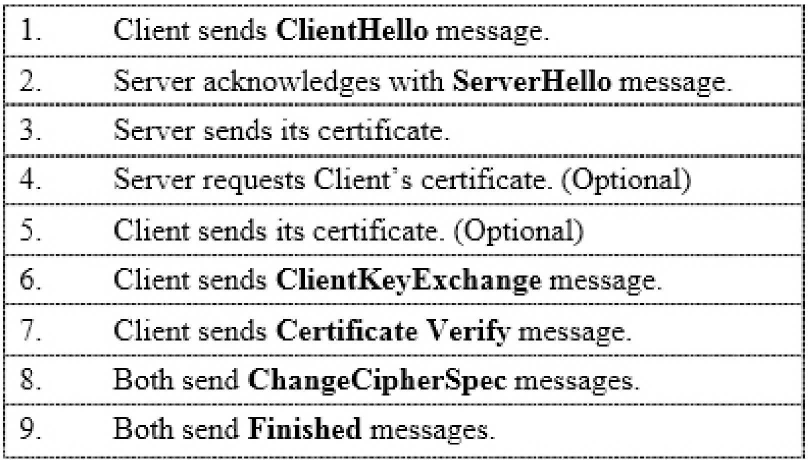
SSL itself is actually composed of three protocols; the Handshake protocol, the Record Protocol and the Alert Protocol. There are discussed briefly in the following sub sections.

2.1 SSL Handshake

During the Handshake Protocol, the following important steps take place: the session capabilities are negotiated, meaning the encryption (ciphers) algorithms are negotiated; and the server is authenticated to the client with the help of a digital certificate, that the server send to the client.

SSL uses symmetric cryptography for the bulk data encryption during the transfer phase; however, asymmetric cryptography, (that is, PKI) is used to negotiate the key used for that symmetric encryption. This exchange is critical to the Handshake Protocol. Note that theserver may optionally ask the client to authenticate itself. However, it isnot necessary to the protocol. Table 1 give the steps of the Handshake Protocol.

Table 1 Handshake Protocol



1.	Client sends **ClientHello** message.
2.	Server acknowledges with **ServerHello** message.
3.	Server sends its certificate.
4.	Server requests Client's certificate. (Optional)
5.	Client sends its certificate. (Optional)
6.	Client sends **ClientKeyExchange** message.
7.	Client sends **Certificate Verify** message.
8.	Both send **ChangeCipherSpec** messages.
9.	Both send **Finished** messages.

2.2 SSL Records

The encryption for all messages in SSL is handled in the Record Protocol. This protocol provides a common format to frame all Alert, Change Cipher Spec, Handshake, and application protocol messages.[1]

SSL records consist of the encapsulated data, digital signature, message types, version, and length. SSL records are 8 bytes long. Because the record length is fixed, encrypted messages sometimes include padding and pad length in the frames.

2.3 SSL Alert Protocol

As mentioned earlier, the Alert protocol handles any questionable packets. If either the server or client detects an error, it sends an alert containing the error. There are three types of alert messages: warning, critical and fatal. Based on the alert message received, the session can be restricted (warning, critical) or terminated (fatal).

3. SSL SECURITY ATTACKS

During the past few years, different attacks were conducted against SSL. Most of them exploit the vulnerabilities of the clients' browsers deploying SSL technology. In the following sub-sections we discuss these attacks and the origin and the conditions for the attacks to happen successfully.

3.1 SSL Sniffing Attack

The origin of this attack is based on vulnerability present in Web Browsers that can be exploited by the attacker. There is a field in the certificates called Basic Constraints. The Basic Constraints field has two parameters; Subject Type and Path Length Constraint. The later parameter indicates the maximum number of CA certificates above the given certificate in the certification path. Path Length Constraint is used to ensure that the holder of the certificate can only issue End Entity certificates and not CA certificates. If the browser did not check this field when it comes to validating a certificate, an attacker can use this certificate to sign a request of a forged certificate. This forged certificate will be treated by Web Browsers as a trusted certificate. When no basic ''constraint field'' validation is done, clients' browsers will consider the chain in the forged certificate as a trusted chain, and hence establish a secure channel with attackers rather than legitimate entities.

Microsoft Internet Explorer 7 and prior versions are vulnerable to the SSL Sniffing Attack. This vulnerability is originated as a result of bypassing the "Basic Constraints" field validation. In this attack an ARP spoofing tool called arpspoof is used to achieve traffic redirection. As a result of using arpspoof, all the traffic between client and server will be redirected to the attacker machine.

When the real server replies back to the real client providing it with its certificate, the attacker intercepts this message taking by this action the client's identity. At this point, the attacker has a secure communication with the server. Now the attacker creates a certificate on the fly imitating the server (a certificate that includes the server information) and signs it with whatever valid certificate it possesses. This newly created and signed certificate is valid because the certificate chaining leads to a valid authentic CA. This certificate is then sent to a client resulting in another secure channel between the client and the attacker. Using the MitM attack and on-the-fly certificate generation, the attacker will open two secure channels, one with the victim, and the other with the legitimate server. At this point all the secure communication is intercepted by the attacker.

3.2 MD5 Collide Certificate Attack

MD5 is a widely used cryptographic hash function and is employed in a variety of security applications. It is supposed to provide the following properties:

- Given message m, it is computationally easy to get the hash h = H(m).
- Given hash h, it is computationally infeasible to get m out of h, such that h = H(m).
- Given m and h = H(m), it is computationally infeasible to get another message n, such that H(n) = H(m). This property is known as collision resistance.

However, it has been shown that MD5 is not collisionresistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on thisproperty [3]. Unfortunately, some CAs still use MD5in SSL certificates and digital signatures, and hence,compromising the security of their clients. Despite thewarnings made in 2004 regarding the danger of MD5collisions, statistics in 2008 showed that 9000 certificatesare still using MD5 rather than SHA1.

To start the attack, the attacker needs a valid legitimate certificate that is signed with a real CA. The certificate should use MD5 and should be accepted by all browsers (let us call this certificate original.cer). One root CA that provides these properties is Equifax Secure Global eBusiness CA-1. Next, the attacker issues a certificate request to be signed by this CA. As expected, the Equifax authority will sign the certificate request and send it back to the client. At this point, the attacker creates another certificate request with crafted information that will help tocause the MD5 collision. However, he does not send the request to a legitimate CA, but rather he uses the same signature digest of the first legitimate certificate (original.cer) and add it to this rogue certificate (say rogue.cer). This rogue certificate is valid over the signature. Anyone who examines the rogue certificate will think that it has been signed by Equifax authority while the fact is that Equifax has never seen this certificate before.

Now, the attacker is in possession of a rogue certificate that can be used to sign other certificates. Since the rogue certificate has been created by the attacker and not by a CA, the attacker sets the Basic Constraints field to TRUE. This means that the attacker is able to use this certificate to sign other leaf certificates. From now on, the attacking scenario will be the same as the scenario described in SSL Sniffing attack discussed in Section 3.1.

All Web Browsers are vulnerable to this attack as long as they accept MD5 hash functions. Unfortunately companies kept using MD5 hash functions. Newer versions of IE including IE9 have not revoked certificates using the MD5 hash function. The best defence against this attack is to use stronger hash functions like SHA1 or SHA2. IE, FireFox v3, Opera Pre v9 and Safari are vulnerable to this attack.

3.3 SSL Stripping Attack

Websites usually use SSL only when transferring confidential data between client and the server. When a user types in an address like www.gmail.com in the address bar, a redirection happens that expands the website address to along URL which is hard to remember otherwise. This is called HTTP 301 permanent redirection.[2] But since this is a secure site, an another redirection happens called HTTP 302 temporary redirection. This redirection means that the connectionsession has been moved temporarily to https://www.google.com/../../../accounts and is ready to accept userinformation in a securemanner.

The attacker can exploit specifically the 302 redirections to let the secure traffic be redirected to his machine instead of forwarding it to the legitimate server. The point where the 302 redirection occurs is the point where an elusive tool called sslstrip [4] can be used to tell the users to navigate http://www.google.com/../../../accounts rather than https://www.google.com/../../../accounts. Notice that this new URL is http and not https. At this point, all the traffic exchanged between the client and the attacker is exchanged in the clear. However, the communication between theattacker and the server is completely legitimate and encrypted using the server's legitimate public key. The server's response will be decrypted by the attacker before forwarding it to the client.

This attack exploits the people's unawareness about secure communication in addition to the HTTP technical vulnerability. This attack can be checked by educating people or more appropriately by adding the https URL into the browser's bookmark. Sowhenever a user would like to access the secure loginwebpage, it will be downloaded into the browser without302 redirections.

3.4 SSL Null Prefix Attack

Null-prefix attack[5] is a silent MitM attack that exploits the treatment of the fields obtained from X509 certificates via most contemporary SSL/TLS implementations, and the signing process of contemporary Certificate Authorities. X509 certificates support PASCAL strings which are represented as a series of bytes mediated by another series of bytes indicating the length of the string followed by the data itself. C strings, on the other hand, are represented as a series of bytes terminated by the NULL character (‘‘\0’’).

When a user submits a Certificate Signing Request(CSR) to the Certificate Authorities, it validates the identity of the owner based on a comparison between the domain listed in the ‘‘common name’’ field retrieved from the request (www.paypal.com\0.attacker.com), and the root domain retrieved by looking up WHOIS database. The identity information is only associated with the root domain, so the CA does not care about the content of the any subdomains that might be present in the users’ requests. Consequently, submitting a request for www.attacker.com or www.paypal.com\0.attacker.com to Verisign does not yield any difference as long as it can prove that you are the owner of attacker.com. Unfortunately, most contemporary SSL/TLS implementations uses ordinary C strings functions for manipulation and comparison and not PASCAL strings. A string comparison between www.paypal.com and www.paypal.com\-0.attacker.com will be identical. Therefore, the owner of www.paypal.com\0.attacker.com certificate can present his certificate for connections intended for www.paypal.com, and thus breaking the authenticity of the intended server.

Figure 9 shows the details of this attack. IE, FireFox, Chrome, Opera and Safari are vulnerable to the attack because of flaws in network security services (NSS) functions as mentioned earlier.

3.5 OCSP Attack

OCSP is a protocol inwhich the browser communicates with a server in real time to determine if a certificate is still trustworthy and notrevoked. Clearly, this process is very time consuming. In addition, it places a burden on the CA’s servers. When the Web Browser is presented a certificate that it has never seen before, the browser contacts the certificate issuer to confirm the validity of the certificate.

OCSP attack is based on exploiting the OCSP response in which it is very hard to revoke Null-prefix certificates described in pervious sub-section.[6] There are actually two structures in an OCSP response message; response Status and response Bytes. In the response Bytes structure, there exists a field that requires the signature of the CA, it is called the BIT STRING field. To forge the OCSP response, the attacker first needs to avoid the ‘‘successful’’ status under the response Statusstructure, since that would require including the CA’ssignature in the response Bytes structure; a signature the attacker cannot obtain. The ‘‘tryLater’’ is used as it doesnot require a signature and does not convey any errorconditions. The attack is based on intercepting OCSP response which for instance is intended for www.paypal.com server, and generating a forged one with response status as ‘‘tryLater’’,which is simply the single ASCII character ‘‘3’’. The userwon’t notice anything and by activating this mode insslsniff tool, it will be very hard to revoke the null- prefixcertificate, thus defeating OCSP [6].

3.6 Change Cipher Spec-Dropping

This attack takes advantage of the lack of protection for change cipher spec messages. We assume the special case where the negotiated ciphersuite includes only message authentication protection and no encryption. The active attacker intercepts and deletes the change cipher spec messages, so that the two endpoints never update their current ciphersuite; in particular, the two endpoints never enable message authentication or encryption in the record layer for incoming packets. Now the attacker allows the rest of the interaction to proceed, stripping off the record layer authentication fields from finished messages and session data. At this point there is no authentication protection for session data in effect, and the active attacker can modify the transmitted session data at will. The impact is that, when an authentication-only transform is negotiated, an active attacker can defeat the authentication protection on session data, transparently causing both parties to accept incoming session data without any cryptographic integrity protection.

The simplest fix is to require that a SSL implementation receive a change cipher spec message before accepting a finished message.

3.7 Key Exchange Algorithm-Spoofing

This attack exploits a design flaw in the SSL 3.0 handshake protocol. A server can send shortlived public key parameters, signed under its longterm certified signing key, in the server key exchange message. Several key-exchange algorithms are supported, including ephemeral RSA and Diffie-Hellman public keys. Unfortunately, the signature on the short- lived parameters does not protect the field which specifies which type of key-exchange algorithm is in use. Note that this violates the Horton principle: SSL should sign not just the public parameters but also all data needed to interpret those parameters.

In the SSL 3.0 data structure from server exchange message we can analyse the signed_params field contains the server's signature on a hash of the relevant ServerParams field, but the signature does not cover the KeyExchangeAlgorithm value. Therefore, by modifying the (unprotected) Key Exchange Algorithm field, we can abuse the server's legitimate signature on a set of Diffie-Hellman parameters and fool the client into thinking the server signed a set of ephemeral RSA parameters.

3.8 Version RollBack

Although most of the Web Browsers and Servers rely on SSL 3.0 for securing the communication, there is a support in almost all the browsers for SSL 2.0. SSL 3.0 have the capability to accept the SSL 2.0 connections. This threatens to create the potentialfor version rollback attacks, where an opponentmodifies the client hello to look like a SSL 2.0 hellomessage and proceeds to exploit any of the numerousSSL 2.0 vulnerabilities.

Paul Kocher designed a fascinating strategy to detectversion rollback attacks on SSL 3.0. Client implementationswhich support SSL 3.0 embed some fixed redundancy in the (normally random) RSAPKCS padding bytes to indicate that they supportSSL 3.0. Servers which support SSL 3.0 will refuse toaccept RSA-encrypted key-exchanges over SSL 2.0 compatibility connections if the RSA encryption includesthose distinctive non-random padding bytes.This ensures that a client and server which both supportSSL 3.0 will be able to detect version rollbackattacks which try to coerce them into using SSL 2.0.Moreover, old SSL 2.0 clients will be using randomPKCS padding, so they will still work with serversthat support SSL 2.0.First, the success of the countermeasure dependsvitally on the assumption that SSL 2.0 will onlysupport RSA key-exchange; non-RSA public keyexchangealgorithms will not admit the specialpadding redundancy, so version rollback attacks cannot be detected if the server supports non-RSA keyexchangemethods while operating in SSL 2.0 mode.All the browsers that support SSL 2.0 are vulnerable.

4. BEAST AND CRIME

BEAST and CRIME are the two very recent attacks discovered by a group of researchers. Although, there is no proof that these attacks have been conducted in a commercial setup or not, they expose some serious fractures in the SSL system to secure web transactions.

4.1 BEAST (Browser Exploit Against SSL/TLS)

BEAST was recently discovered by a group of researchers and it exploits a vulnerability that reside in SSL 3.0 and versions 1.0 and earlier of TLS, the successor of SSL. Although versions 1.1 and 1.2 of TLS aren't susceptible, they remain unsupported in many web browsers and websites. BEAST uses a piece of JavaScript Code that works with a network sniffer to decrypt the encrypted cookies a targeted website uses to grant access to restricted user accounts. The exploit works even against HSTS, or HTTP Strict Transport Security, which prevents certain pages from loading unless they're protected by SSL.BEAST attack was mitigated by reconfiguring web servers to use theRC4 cipher-suite rather than AES. But the newer attack CRIME enables miscreants to run in man-in-the-middle-style attacks and is not dependant on cipher-suites.

4.2 CRIME(Compression Ratio Info-leak Made Easy)

After BEAST was mitigated, discoverers of BEAST came up with a new attack called CRIME. All versions of TLS/SSL – including TLS 1.2, on which theBEAST attack did not work – are vulnerable. The researchers say that once they have placedthemselves in the middle of a given network, they can sniff the HTTPS traffic and launch theattack. Their chosen way to get that position is by running JavaScript code in the victim'sbrowser, but the attack doesn't rely on JavaScript.The cipher suite doesn't matter, say the researchers, noting that one workaround for BEASTattacks was to switch from AES to RC4, but for CRIME that isn't important. The feature thatCRIME is leveraging for its attack has, they say, not been a major subject for security researchin the past, but for the attack to work it must be supported at the client and server.

5. CONCLUSION

SSL has been long known for securing all the communication traffic between the client and server, thus preventing attackers from tampering with data during transition. However, improper design of SSL in the various applications could lead to unexpected consequences. The above discussed attacks exploit the design flaws of SSL.

REFERENCES

1. *SSL and TLS Essentials: Securing the Web (p. 69) Thomas*
2. *Network Working Group. Hypertext Transfer Protocol(HTTP/1.1) RFC, June 1999.*
3. *Wang X, Yu H. How to break MD5 and other Hashfunctions, Eurocrypt 2005, Lecture Notes in ComputerScience, vol. 3494, May 2005; pp. 19-35.*
4. *Moxie M. SSLStrip: http://www.thoughtcrime.org/software/sslstrip*
5. *Marlinspike M. Null prefix attacks against ssl/tlscertificates, 29/7/2009, http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf.*
6. *Marlinspike M. OCSP attack, 29/7/2009, http://www.thoughtcrime.org/papers/ocsp- attack.pdf*
7. *Stevens M, Sotirov A, Appelbaum J, et al. ShortChosen-Prefix Collisions for MD5 and the Creationof a Rogue CA certificate, Proceedings of CRYPTO2009, to appear*

Energy- Efficient Position based Routing Protocol using Back Pressure Technique for Mobile Ad Hoc Networks

Supriya Srivastava* , A K Daniel*
*Computer Science & Engineering Department, M M M Engineering College,
Gorakhpur, U. P., India

ABSTRACT

A mobile Ad-Hoc network is an infrastructure less temporary network without any centralized administration. In such network, all nodes are mobile and can be connected dynamically in an arbitrary manner. In mobile Ad-Hoc networks, limited power supply is a challenge. So energy efficient mechanisms should be combined with existing routing protocols to reduce node failure and improve the network lifetime. This paper presents an Energy-Efficient Position Based Routing protocol (EEPBR) using Backpressure technique for Mobile Ad Hoc Networks. The protocol deals with four parameters as Residual Energy, Bandwidth, Load and Hop Count for route discovery. The problem of the link failure in the channel during the call in progress thus leads to the degradation of the QoS (Quality of Service). To deal this we are using a Backpressure Technique. The simulation results show that the proposed algorithm is able to find a better solution, fast convergence speed and high reliability. The simulation results shows that the proposed EEPBR protocol achieve the above objectives and gives the better results than previous schemes like DSR. Our proposed scheme is useful for minimizing the overheads, maintaining the route reliability and improving the link utilization.

Keywords: Bandwidth, Load, MANET and Residual Energy.

1. INTRODUCTION

Mobile ad hoc network is a collection of mobile devices which can communicate through wireless links. The task of routing protocol is to direct packets from source to destination. This is particularly hard in mobile ad hoc networks due to the mobility of the network elements and lack of central control. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which it forwards the packet; the sender explicitly lists this route in the packet's header, identifying each forwarding “hop” by the address of the next node to which to transmit the packet on its way to the destination host. Source routing has been used in a number of contexts for routing in wired networks, using either statically defined / dynamically constructed source routes. The protocol presented here is explicitly designed for use in the wireless environment of an ad hoc network. When a host needs a route to another host, it dynamically determines one based on cached information and on the results of a route discovery protocol. Dynamic source routing protocol offers a number of potential advantages over conventional routing protocols such as distance vector in an ad hoc network. Source routing is a technique in which the source node determines the entire sequence of nodes through which a packet has to pass. The source node puts the list of addresses of all nodes in the header of the packet, so that the packet is forwarded to the destination through those specified nodes. However source routing can be done statically or dynamically. Here it does dynamically. This is done using a procedure called route discovery. Whenever a node has packet to send to some other node, the first node initiates the route discovery. Each node maintains a cache called route cache to store the routes it has gathered to different destinations. To support efficient routing in energy constrained ad hoc networks, power-aware routing policies can be integrated and evaluated with existing features of routing protocol. Unlike conventional routing protocols, our protocol uses no periodic routing advertisement messages, thereby reducing network bandwidth. The proposed protocol enhances Dynamic Source Routing protocol with some Energy constraints to improve its performance [1] [12]. As the residual energy of nodes in an ad hoc network goes below threshold, some of the existing links break and the routes in the route caches of the nodes must be modified and alternative route may be used. The rest of the paper is organized as follows: we have given design space and related works in Section 2, Section 3 presents the proposed protocol, Section 4 discusses Simulation results and finally Conclusion and Future work is discussed in Section 5.

2. DESIGN SPACE AND RELATED WORK

The routing concept basically involves two activities first, determining optimal routing routes and secondly, transferring the information packets through network. There are various Energy-Efficient routing protocols which deal with the following constraints:

- Switching on/off radio transmitters to conserve energy [2][3],
- Power and topology control by adjusting the transmission range (power) of transmitters [4][5],
- Routings based on the energy efficient metrics [6][11].

The radio transmitters are turned off for an adaptively varying period to save power when there is no traffic [2]. In order to adapt to operational environment, several algorithms are proposed, for examples, using application level information and node density [2], and routing fidelity and location information [3]. Topology control is another approach, in which the transmission power is adjusted to achieve energy efficiency. For instance, the transmission power is changed while maintaining a connected topology by observing local and global topology information [4]. The node battery life is extended by using the radio's minimum power level. A distributed power control scheme is proposed, in which power control level is established by exchanging control messages, according to the estimated minimum and maximum power level [5]. There will be frequent link ups and downs, causing more link errors. Retransmission due to link breakage will consume extra energy and network bandwidth. For Metric-based routing [6] [7], different kinds of metrics are used to maximize the lifetime of networks by evenly distributing the energy consumption among all nodes. MBCR (Minimum Battery Cost) algorithm incorporates the battery capacity into the metric. In addition, the expected energy spent in reliably forwarding a packet over a specific link is considered in [8] [11]. In order to maximize the network life time, the cost function defined in [9] takes into account energy expenditure for one packet transmission and available battery capacity. Furthermore in [10], the queue load condition and the estimated energy spent to transmit all packets in the queue are considered.

2.1 Dynamic Source Routing Protocol (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol. Mobile nodes are required to maintain route caches that contain unexpired routes and are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance.Route Discovery is done by the source if it doesn't found any route for the destination in its route cache. It is done by broadcasting a RREQ packet to all the neighbors initiated by source then by every node that receives the RREQ packet, till the destination is found. When destination receives a RREQ packet, it replies source with a RREP packet along the reverse of the route recorded in RREQ. Route maintenance: Route maintenance is done by the use of route error packets and acknowledgments. RERR packet is send by a node to the source when the data link layer met a fatal transmission problem. When a RERR packet is received, the erroneous hop is removed from the node's route cache and all routes that contain that hop are truncated at that point [6].

3. PROPOSED ENERGY EFFICIENT ROUTING PROTOCOL

DSR is selected as the baseline routing protocol because it is an On-Demand routing protocol. It consists of two main phases: Route Discovery and Route Maintenance. Consider a Mobile Ad-Hoc network (MANET) with a collection of mobile nodes connected with each other through some routes shown in Fig 3.

3.1 Proposed Model for Route Discovery

The specific goal of this approach is to select a route that contain underutilized nodes so that the energy usage among all nodes can be balanced because underutilized nodes usually have more energy than utilized nodes. The approach compares not only energy but other parameters also for the route selection so this may result in shorter, best and energy-rich routing. Thus, ensures longevity of network lifetime.

Route Discovery: In this protocol the procedure of broadcasting the RREQ packet for Route Discovery is same as the DSR; the difference is in the RREQ packet format, shown in fig1:

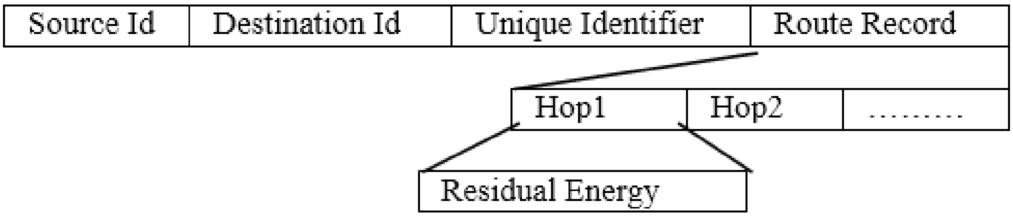


Fig 1. RREQ packet format

The intermediate node which receives the RREQ packet does the following:

a) It checks in its Route Cache for the existence of a route for the destination, if found it appends that route in a RREP packet and sends it to the source.

b) If the node had already received the request with the same Unique Identifier, it drops the arrived request packet.

c) If the node recognizes its own address as the Destination, then the packet reached the target.

d) Otherwise, the node appends its own address in the Route Record and its residual energy in RREQ and rebroadcasts it to all its neighbors.

The destination selects the best route on the basis of different parameters like max Energy, max Bandwidth, min Load and min Hop Count among the entire route requests arrived. The destination replies to the source by sending a RREP packet (Fig. 2). The RREP packet goes along the reverse hop sequence of the best route and also contains the Final Route Table (Table 4). The Final Route Table is saved by each intermediate node and the source node in its route cache. The RREP packet format will be as

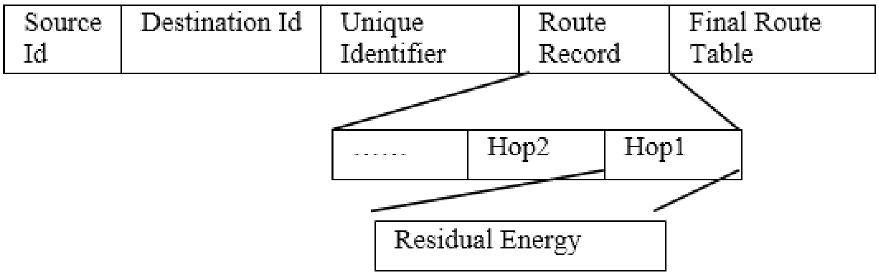


Fig 2. RREP packet format

3.2. Proposed Algorithm and Analysis

Let us consider few parameters as for a MANET shown in Fig 3:
H = Hop Count i.e. no. of edges in a route between source and destination
Dij = Distance between any two nodes i and j
L = Load at a node
BW = Available Bandwidth at each node
E = Energy at each node

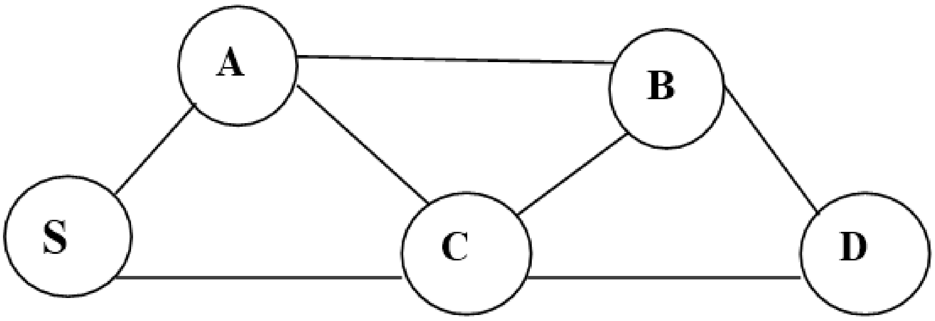


Fig 3. A mobile Ad-Hoc network

Table 1 show the total number of routes available between source S and Destination D with their Hop Count are:

Table 1: Routes with their Sequence and Hop Count

Routes	Complete Route Sequence	Hop Count
R1	S - A - B – D	3
R2	S – C – D	2
R3	S – A – C – B – D	4
R4	S – C - B – D	3
R5	S – A - C – D	3
R6	S – C – A – B – D	4

The load at the each node (Traffic Load) is:
L(S)=30, L(A)=10, L(B)=15, L(C)=20, L(D)=25

The Bandwidth of each node is:
BW(S)=40, BW(A)=25, BW(B)=20, BW(C)=30, BW(D)=35

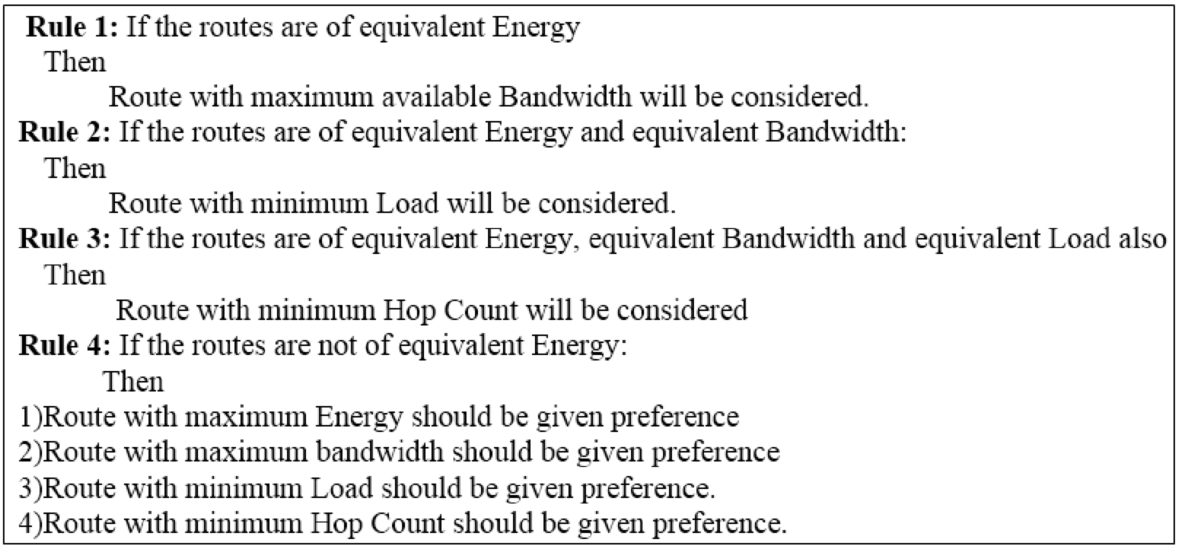
The Energy of each node is:
E(S)=45, E(A)=40, E(B)=35, E(C)=30, E(D)=25

Now combined representation of all the routes with minimum possible values of all the parameters on each route is shown in Table 2.

Table 2: Minimum Value of all Parameters in each Route

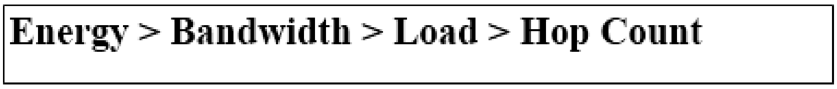
Routes	Load	Bandwidth	Energy	Hop Count
R1	10	20	35	3
R2	20	30	30	2
R3	10	20	30	4
R4	15	20	30	3
R5	10	25	30	3
R6	10	20	30	4

For choosing an optimal route, following Rule Set should be taken into account:



Rule 1: If the routes are of equivalent Energy
Then
Route with maximum available Bandwidth will be considered.
Rule 2: If the routes are of equivalent Energy and equivalent Bandwidth:
Then
Route with minimum Load will be considered.
Rule 3: If the routes are of equivalent Energy, equivalent Bandwidth and equivalent Load also
Then
Route with minimum Hop Count will be considered
Rule 4: If the routes are not of equivalent Energy:
Then
1)Route with maximum Energy should be given preference
2)Route with maximum bandwidth should be given preference
3)Route with minimum Load should be given preference.
4)Route with minimum Hop Count should be given preference.

The preference order for selecting optimal route is as follows



Energy > Bandwidth > Load > Hop Count

Now tabular arrangement of the routes on the basis of above rule set and their positions is shown in Table 3:

Table 3: Position Based Arrangement of all Routes

Position	Hop Count	Load	Bandwidth	Energy
1	R1	R2	R2	R1
2	R3	R1	R5	R2
3	R5	R4	R1	R3
4	R6	R5	R3	R4
5	R4	R3	R4	R5
6	R2	R6	R6	R6

Now calculating the sum of positions of routes for all the different parameters (Hop Count, Load, Bandwidth and Energy) shown in Table3:

For R1: 1+2+3+1 = 7
For R2: 6+1+1+2 = 10
For R3: 2+4+4+3 = 14

For R4: 5+3+5+4 = 17
For R5: 3+4+2+5 = 14
For R6: 4+6+6+6 = 22

Now the Final Route Table (FRT) that will suggest the best and all the alternative routes:Table 4: Final Route table

S. No.	Routes	Complete sequence	Position Count
1	R1	S - A - B – D	7
2	R2	S – C – D	10
3	R3	S – A – C – B – D	14
4	R5	S – A - C – D	14
5	R4	S – C - B – D	17
6	R6	S – C – A – B – D	22

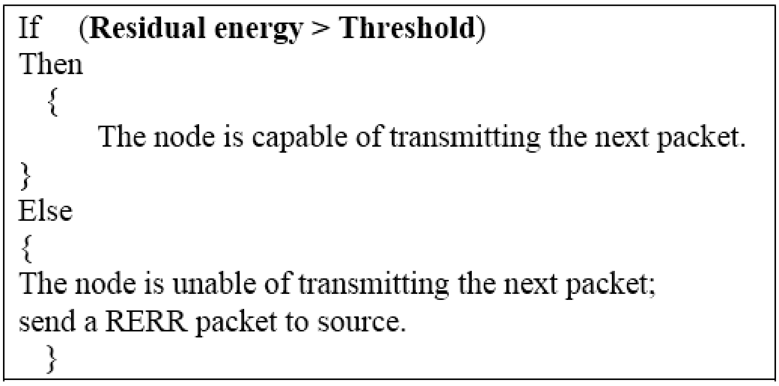
From the Table 4, it is clear that the position count for route R1 is lowest. So R1 will be selected as the best route for sending data packets and the remaining routes will be used as backup routes. This table is send to the source node and will be used to select alternate routes for sending data packets whenever a link failure occurs in current route.

3.3 Route Maintenance Model

The Route maintenance is required when residual energy of any node goes below the threshold. After each transmission of packet, the energy factor is computed.

Energy consumed in one Transmission = (Available Energy before transmission - Remaining Energy after transmission)

The energy available for next transmission is computed as
Residual energy = (Remaining Energy after transmission - Energy consumed in one transmission)

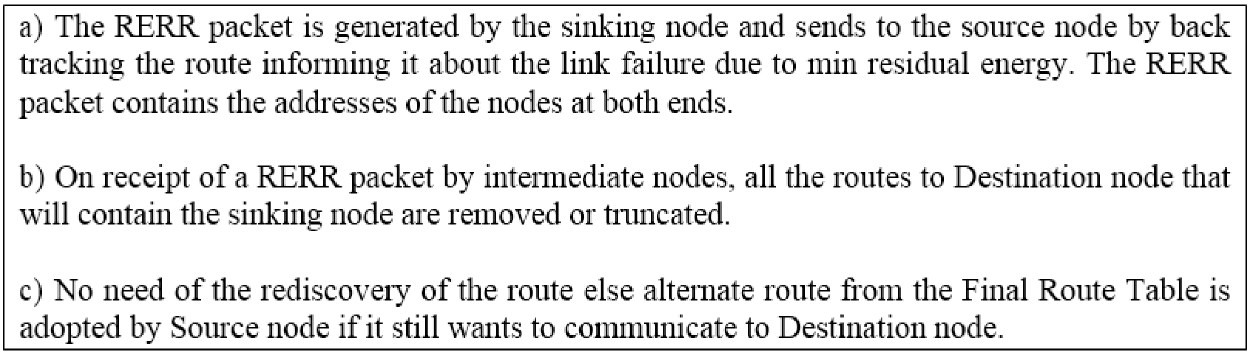


```
If    (Residual energy > Threshold)
Then
   {
        The node is capable of transmitting the next packet.
}
Else
{
The node is unable of transmitting the next packet;
send a RERR packet to source.
   }
```

If any node tries to send the packet even when its energy is below threshold of the required energy then data packet will definitely be lost.

3.3.1 Proposed model using Back pressure technique for Route Maintenance

The Route maintenance procedure monitors the operation of a route in use and informs the source of any routing errors. When any node detects that its energy is not sufficient and it is not capable of transmitting the next packet resulting in link failure then in such condition following steps will take place.



a) The RERR packet is generated by the sinking node and sends to the source node by back tracking the route informing it about the link failure due to min residual energy. The RERR packet contains the addresses of the nodes at both ends.

b) On receipt of a RERR packet by intermediate nodes, all the routes to Destination node that will contain the sinking node are removed or truncated.

c) No need of the rediscovery of the route else alternate route from the Final Route Table is adopted by Source node if it still wants to communicate to Destination node.

Thus, the communication between source node and destination will not face link failure and time delay in next transmission of data packet (between the same source and destination) due to the loss of node's energy.

3.5 Validation and Testing

Case 1: Let us consider above network and the route selected as R1 (S - A - B – D) for sending data packet, the residual energy of the node B is less than Threshold then B generates a RERR packet and send it to its predecessor which forward it to its predecessor and so on, till RERR reaches to the source. The source node truncate all the routes in its Final Route Table that will contain node B and updates this table with all possible alternate routes that will not contain node B for sending the next data packet. The updated Final Route Table is shown in Table 5. Now table 5 show that route R2 has the lower position count than R5, so R2 will be chosen as the alternate route, thus preventing the network failure.

Table 5: Table with alternate routes without node C

S. No.	Routes	Complete sequence	Position Count
1	R2	S – C – D	10
2	R5	S – A - C – D	14

Case 2: Let us Consider Case 1, after transmission of a data packet, if residual energy of node C of route R2 (Table 5) become less then threshold, then it will send a RERR packet to its predecessor node S. Now S will check table 5 for alternative routes that will not contain node C, but no such route exist. Then in this case, source S will rediscover the routes by retransmitting the CTS/RTS.

4. SIMULATION RESULT

The performance of the protocol is evaluated using simulation experiments with C++, Ns-2 simulator with Mobility Framework. A flat network is assumed as clusters Networks. A Nodesends a packet, to set RTS (Request-to- Send) flags of its neighbors and the intended receiver sets CTS (Clear-to-Send) flags of its neighbors. Nodes whose RTS or CTS flag is set cannot transmit data, except the sender. Control packets have higher priority over data packets in simulations, Propagation delay is assumed to be negligible, and it is assumed that packets always arrive without any bit error. The source Node generates packets at a constant rate. Extensive simulation results obtained by varying several network parameters and workload configuration. The values of the network parameters used in simulations are those specified in the IEEE 802.11. We evaluate the performance improvement in terms of throughput due to the use of a densely populated network. Specifically, we consider a network of 5 to 40 Nodes with an increasing number of neighbors from 5 to 10 nodes. Each Node has a traffic flow with infinite demands towards one of its neighbors. Fig 4, Fig 5 and Fig 6 shows the throughput of all traffic flows, with available Energy and Channels Bandwidth.

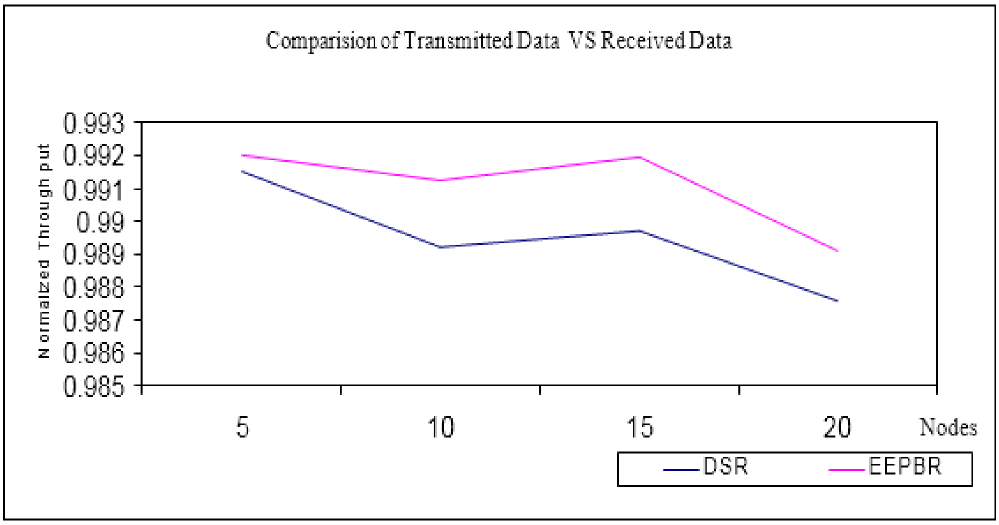


Fig 4. Comparison of Transmitted data with Received data

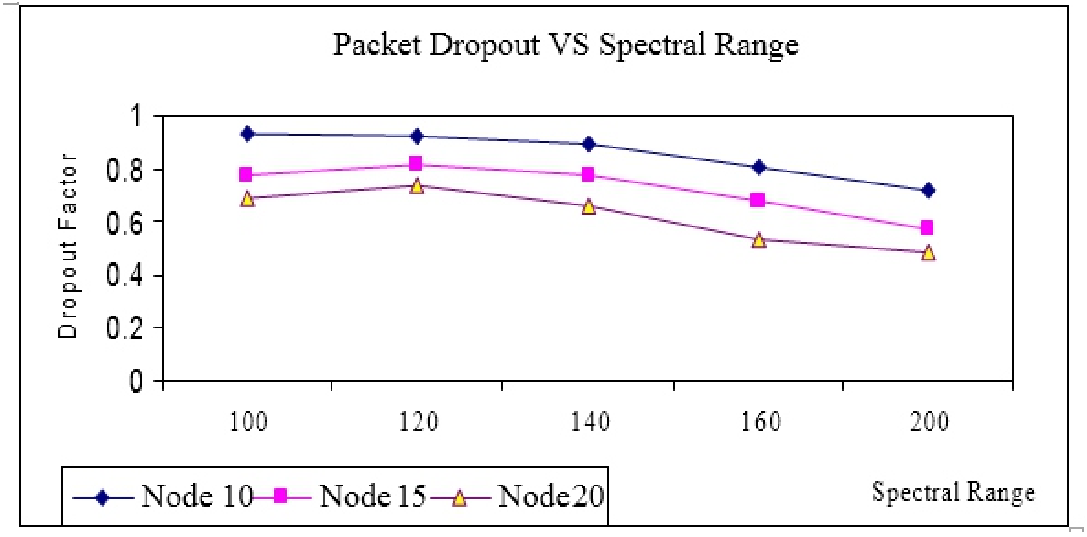


Fig 5. Comparison of Packet Dropout with Spectral Range

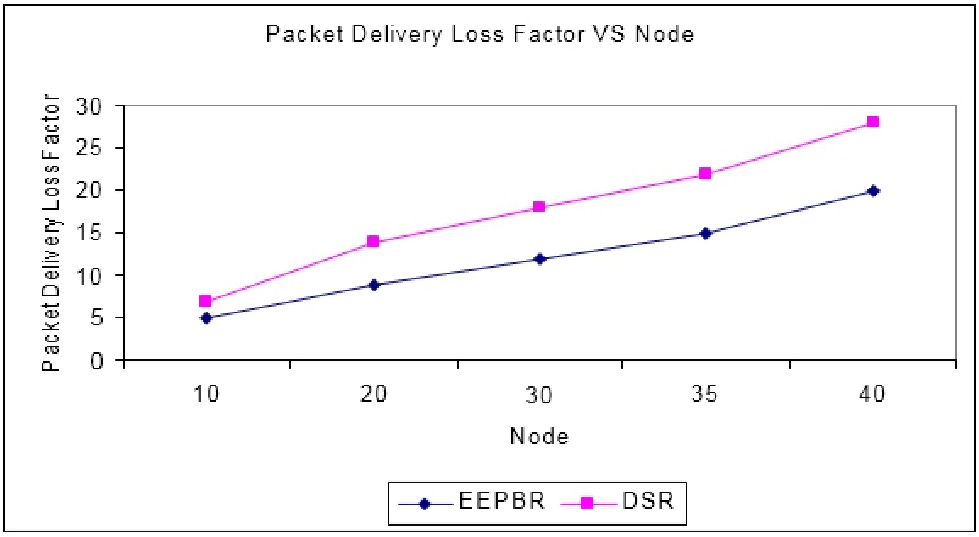


Fig 6. Comparison of Packet Delivery loss factor with node

5. CONCLUSION

The proposed energy efficient routing protocol works on DSR minimizes the overhead of source of rediscovering the routes whenever a network failure occurs due to a node's mobility or a node's failure by providing alternative route information to the source node and giving it a control of selecting the alternative route. It reduces network failure due to loss of node's energy and minimizes loss of data packets. It also balances the consumption of energy between utilized nodes and the underutilized nodes.

6. REFERNCES

[1] Y. Xu, J. Heidemann and D. Estrin, "Geography-informed energy conservation for ad hoc routing," Proceedings of the 7th Annual ACM Mobicom, 2001.

[2] Y. Xu, J. Heidemann and D. Estrin, "Adaptive energy-conserving routing for multihop ad hoc networks," Technical Report TR-2000-527, 2000.

[3] Y. Xu, J. Heidemann and D. Estrin, "Geography-informed energy conservation for ad hoc routing," Proceedings of the 7th Annual ACM Mobicom, 2001.

[4] Ramanathan and Rosales-Hain, "Topology control of multihop wireless networks using transmit power adjustment," IEEE Infocom 2000.

[5] P. Bergamo, D. Maniezzo, A. Giovanardi, G. Mazzini, and M. Zorzi, "Distributed power control for power-aware energy-efficient routing in ad-hoc networks," Proceedings of European Wireless 2002 Conference, Feburary 2002.

[6] S. Singh, M. Woo and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," Proceedings of MobiCom 1998, 1998.

[7] C. K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," IEEE Communication Magazine, 2001.

[8] Archan Misra, Suman Banerjee, "MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments," IEEE Wireless Communications and Networking Conference (WCNC) 2002, March 2002.

[9] J. H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad hoc networks," IEEE Infocom 2000, March 2000.

[10] K. Kalyan kumar and A. Chockalingam, "Energy Efficient Routing in Wireless Ad-hoc," Proceedings of National Conference on Communications 2002, January 2002.

[11] Carla F. Chiasserini, Pavan Nuggehalli and Vikram Srinivasan, "Energy-Efficient Communication Protocols," Proceedings of 39th Design Automation Post-Conference (DAC) 2002, June 2002.

[12] Ramanathan and Rosales-Hain, "Topology control of multihop wireless networks using transmit power adjustment," IEEE Infocom 2000.

Zone Routing Protocol (ZRP) in AD-HOC Networks

Sweety Goyal*

*Lecturer, Department of Computer Science & Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar University, Mullana, Ambala (Haryana)

ABSTRACT

Routing protocols for wireless ad-hoc networks face the challenge of dynamic topology due to node mobility, limited channel bandwidth and low transmission power. Both proactive and reactive protocols have trade-off in them. Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. The ZRP is a hybrid protocol that overcomes the shortcomings of both proactive and reactive routing protocol. ZRP divides the entire network into overlapping zones of variable size where routing inside the zone is performed using proactive approach and outside the zone is performed using reactive approach.

Keywords: Ad-hoc Networks, Routing, Reactive, Proactive, ZRP.

1. INTRODUCTION

Ad-hoc networks are wireless networks that have no fixed infrastructure. They are characterized by dynamic topology with no fixed routers. These networks are gaining popularity within the computing industry for their attractive features and applications. Many more applications exist already or are imaginable in the near future as it is expected that ad- hoc networking will be more intensively used for different applications such as digital battlefield communications, movable base-stations, and range extension for cellular telephone [4].

One of the most demanding and challenging aspects of ad-hoc networks is the routing issue. Routing can be defined as the process of finding a path from the source to the destination to deliver packets to the destination nodes while the nodes in the network are moving freely [4]. Secure routing is also a vital factor for mobile ad-hoc networks because of the sensitive applications of these networks. However, achieving security goals, such as confidentiality, authentication, integrity, availability, and access control in these networks is a challenging task. In general, a mobile ad-hoc network is particularly vulnerable to attacks due to its fundamental characteristics of open medium, dynamic topology, distributed cooperation, constrained capability, and absence of central authorities [5].

2. ROUTING IN AD-HOC NETWORKS

Routing in ad-hoc networks is the process of selecting paths in a network by which a packet travels from a source to a destination. The nodes which are in the transmission range of each other communicate directly otherwise communication is done through intermediate nodes. Thus each node may act as router or as host. Depending on how node establish and maintain a route to the destination, protocols can be classified into three categories: proactive (table driven), reactive (demand driven), hybrid routing protocols.

2.1 Proactive Routing

Proactive approach is a table driven protocol where each node maintains consistent up-to-date information to every other node in the network by maintaining routing table(s). Therefore a routing path is known and is immediately available to the source node if it needs one. Using a proactive routing protocol nodes continuously calculate routes to all nodes that are reachable and thus maintains a consistent view of topology. Some of the proactive routing protocols are:

- DSDV
- WRP
- OLSR
- FSR

Proactive protocols have the advantage of minimum initial delay but causes significant signaling traffic and power consumption problem. These protocols results in a large overhead due to the route maintenance and frequent route updates.

2.2 Reactive Routing

Reactive routing protocols are on-demand protocols where routing information is acquired only where it is needed. In reactive routing, a route determination process is invoked on demand when a node request for a route. The reactive routing protocols do not maintain the information about the routes; rather routes are maintained only during the communication or for some period of time. Some of the reactive routing protocols are:

- AODV
- DSR

Reactive routing adds latency to the network due to the route discovery mechanism. These protocols decrease the routing overhead but at the cost of increased latency.

2.3 Hybrid Routing

Hybrid protocol combines the advantage if both proactive and reactive routing protocol. Hybrid protocol is presented to overcome the shortcomings of both Proactive and Reactive protocol. It uses the route discovery mechanism of proactive protocol. Some of the hybrid routing protocols are:

- ZRP
- SHRP

3. ZONE ROUTING PROTOCOL

Zone routing protocol uses the hybrid approach for routing. It uses the advantages of both proactive and reactive protocol. ZRP [2] aims to address excess bandwidth and long route request delay of proactive and reactive routing protocols. ZRP divides the entire network into zones of variable size. Every node in the network has a zone associated to it. The size of a zone is not determined by geographical measurement but is given by a radius of length ρ, where ρ is the number of hops to the perimeter of the zone. ZRP is not a very distinct protocol; it provides a framework for other protocols [1].

4. ZRP ARCHITECTURE

In zone routing protocol, a routing zone is defined for each node separately and the zones of neighboring nodes overlap [2]. The routing zone has a radius ρ expressed in hops. The zone thus includes the nodes, where distance from center node is at most ρ hops. A routing zone with radius two can be seen in figure 1, where the routing zone of S includes nodes A-K but not L.

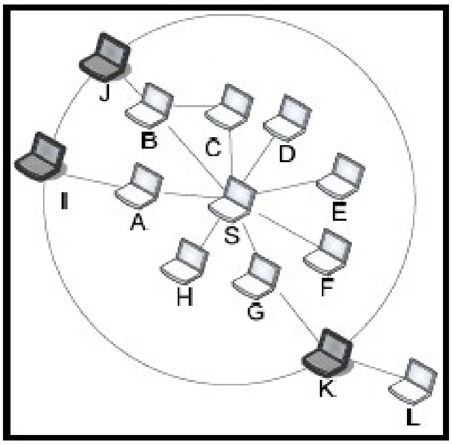


Fig.1 Routing Zone with radius, ρ=2

In figure 1, the nodes A-H are interior nodes, the nodes I-K are peripheral nodes and node L is outside the routing zone. Node J can be reached by two paths, one with length 2 hops through B and one with length 3 hops through C and B. The node is within the zone, since the shortest path is equal to the zone radius.

ZRP uses proactive approach for routing inside the zone i.e. intra-zone routing protocol (IARP) and reactive approach for routing outside the zone i.e. inter-zone routing protocol (IERP).

The Architecture of ZRP is illustrated in Figure 2.

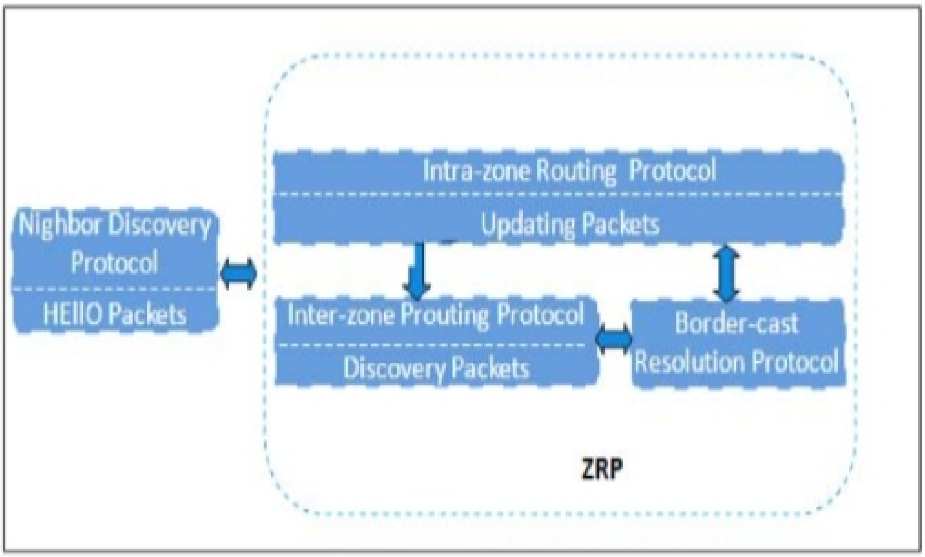

Nighbor Discovery Protocol
HEllO Packets
Intra-zone Routing Protocol
Updating Packets
Inter-zone Prouting Protocol
Discovery Packets
Border-cast Resolution Protocol
ZRP

Fig.2 ZRP Architecture

4.1 Intra Zone Routing Protocol (IARP)

IARP is used by a node to communicate with the interior nodes of its zone and is limited by the zone radius [6]. It maintains routes inside the zone, each node continuously needs to update the routing information in order t determine the peripheral nodes as well as maintain a map of which nodes can be reached locally.

4.2 Inter Zone Routing Protocol (IERP)

IERP is used to communicate between nodes of different zones. It is reactive routing component which offers enhanced route discovery [7]. The IERP needs to be able to take advantage of the local connectivity provided by IARP. Route discovery is done through a process called bordercasting that uses a Bordercast Routing Protocol (BRP) to only transmit route requests to peripheral nodes.

4.3 Bordercast Routing Protocol (BRP)

BRP is used to direct the route requests initiated by the IERP to the peripheral nodes and also utilizes the topology information provided by IARP to construct a bordercast tree. For route requests away from areas of network, a query control mechanism is employed by BRP. [8]

5. ROUTING IN ZRP

In the route discovery mechanism the source initiates the route discovery, it first checks whether the destination is inside or outside the zone [9]. If the destination node is within the zone, the packet is routed using proactive approach and if the destination node is outside the zone, reactive routing is used.

Reactive approach for routing the packet to the destination outside the zone includes two phases: route discovery phase and route reply phase. In route discovery phase, using Bordercast Resolution Protocol (BRP), the source node sends a RREQ (route request) packet to its peripheral nodes. If the node receiving the RREQ packet knows the destination send s a route reply to the source, otherwise the process continues by bordercasting the packet. A node that can provide a route to the destination node sends a route reply to the source node.

6. QUERY CONTROL MECHANISMS

Bordercasting can be more efficient than flooding, since route request packets are only sent to the peripheral nodes and thus only on the corresponding links. However, each node may forward route requests several times due to overlapping zones which results in more traffic than in flooding. The excess traffic is a result from queries returning to covered nodes as in traditional flooding [2].

ZRP uses query control mechanisms, query detection, early termination and random query processing delay to solve this problem. In query detection mechanism, it is possible to detect queries relayed by other nodes in the same zone to prevent them from reappearing in the covered zone. Also, a node can prevent route request from entering already covered regions by using early termination. The information obtained through query detection combined with the knowledge of the local topology can be used to prune bordercasting to peripheral nodes inside covered regions.

Finally, a random query processing delay can be employed to reduce the probability of receiving the same request from several nodes. Each broadcasting node waits a random time before the construction of the bordercast tree and the early termination. During this time the waiting node can detect queries from other bordercasting nodes and prune the bordercast tree [9].

7. CONCLUSION

Zone routing protocol is targeted for large networks that combines the proactive and reactive approach in one protocol. Inside the routing zone, proactive component IARP maintains the routing tables. Outside the zone, route discovery mechanism is done by reactive component IERP using route requests and route replies. A bordercasting process is used for oute discovery using Bordercasting Resolution

Protocol (BRP). To reduce the amount of query traffic, query control mechanisms query detection and early termination can be used. ZRP rather than a distinct protocol, can be taken as routing framework.

REFRENCES

[1] T.Ravi Nayak, Sake Pothalaiah and K Ashok Babu, " Implemntation of Adaptive Zone Routing Protocol For Wireless Networks", IJEST, vol.2 (12), 2012.

[2] Haas, Zygmunt J., Pearlman, Marc R.: The Performance of Query Control Schemes for the Zone Routing Protocol, August 2001, IEEE/ACM Transactions on Networking, Vol. 9, No. 4

[3] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks", Ad Hoc Networks, 2003, v.1, pp.175– 192.

[4] A. M. Kamal, "Adaptive Secure Routing in Ad Hoc Mobile Network," M.S. Thesis, Dept. Computer and Systems Science, Royal Institute of Technology, Stockholm, Sweden, 2004.

[5] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," In Proc. ACM Workshop on Wireless Security, San Diego,WiSe, California, September 2003.

[6] Z.J. Haas, M. R. Pearlman, and P. Samer, "Intrazone Routing Protocol (IARP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-iarp- 01.txt.

[7] Z.J. Haas, M. R. Pearlman, and P. Samer, "Interzone Routing Protocol (IERP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-ierp- 01.txt.

[8] Z.J. Haas, M. R. Pearlman, and P. Samer, "The Bordercast Resolution Protocol (BRP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf- MANETsbrp- 01.txt.

[9] Z.J. Haas, M. R. Pearlman, and P. Samer, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft, 2003, available at:http://tools.ietf.org/id/draft-ietf- MANETs-zone-zrp-04.txt.

[10] Robinpreet Kaur aand Mritunjay Kumar Rai, " A Novel Review on Routing Protocols in MANETs", UARJ, Volume-1, 2012.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005