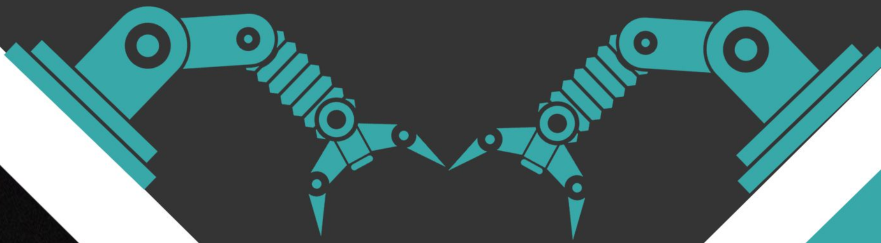
TECH -TALK

THE BIANNUAL MAGAZINE OF COMPUTER SCIENCE AND ENGINEERING



2015-16 ISSUE - I

Computer Science & Engineering Department

VISION

“The Computer Science & Engineering aims at providing continuously stimulating educational environment to its students for attaining their professional goals and meet the global challenges.”

MISSION

- To develop a strong theoretical and practical background across the computer science discipline with an emphasis on problem solving.
- To inculcate professional behavior with strong ethical values, leadership qualities, innovative thinking and analytical abilities into the student.
- Expose the students to cutting edge technologies which enhance their employability and knowledge.
- Facilitate the faculty to keep track of latest developments in their research areas. Encourage the faculty to foster the healthy interaction with the industry.

UG – B.TECH

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

PEO I: To inculcate the adaptability skills into the students for software design, software development or any other allied fields of computing.
PEO II: To equip the graduates with the ability to analyze, design and synthesize data to create novel products.
PEO III: Ability to understand and analyze engineering issues in a broader perspective with ethical responsibility towards sustainable development.
PEO IV: To empower the student with the qualities of effective communication, team work, continues learning attitude, leadership needed for a successful computer professional.

PROGRAMME OUTCOMES (Pos)

Engineering Graduates will be able to:-

Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

Problem analysis: Identify, formulate, review research literature, and analyze complexen gineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

Design/development of solutions: Design solutions for complex engineering problems anddesign system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

Modern tool usage: Create, select, and apply appropriate techniques, resources, and modernen gineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

The engineer and society: Apply reasoning informed by the contextual knowledge to assesssocietal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

Environment and sustainability: Understand the impact of the professional engineering solutionsin societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms ofthe engineering practice.

Individual and team work: Function effectively as an individual, and as a member or leader indiverse teams, and in multidisciplinary settings.

Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

Project management and finance: Demonstrate knowledge and understanding of theengineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES(PSOs):-

1. Programming Paradigms:

To inculcate algorithmic thinking, formulation techniques and visualization, leading to problem solving skills using different programming paradigms.

2. Data Engineering:

To inculcate an ability to Analyse, Design and implement data driven applications into the students.

3. Software Engineering:

Develop an ability to implement various processes / methodologies /practices employed in design, validation, testing and maintenance of software products.

PG - (M.TECH)

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

1. To inculcate the investigating and adaptability skills into the students to carryout research on recent trends in Computer Science and Engineering Technology .

2. To empower the student with the qualities of effective communication, technical document writing, team work, lifelong learning attitude,and leadership needed for a successful career.

3. Enlighten the students on analysing engineering issues in a broader perspective with ethical responsibility towards sustainable development to satisfy the societal needs.

4. Equip the students with all-round knowledge to adapt the evolving technical challenges and changing career opportunities in par with global competency.

Program Outcomes PG Graduates will be able to :-

PO1: Independently carry out research /investigation and development work to solve practical problems

PO2: Write and present a substantial technical report/document

PO3:Demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: Design and develop software projects given their specifications and within performance and cost constraints.

PO5: An ability to Work on multi-disciplinary projectsand exhibit team skills to upgrade knowledge for adoption of current technological changes.

PO6: Understand the impact of the professional engineering solutionsin societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

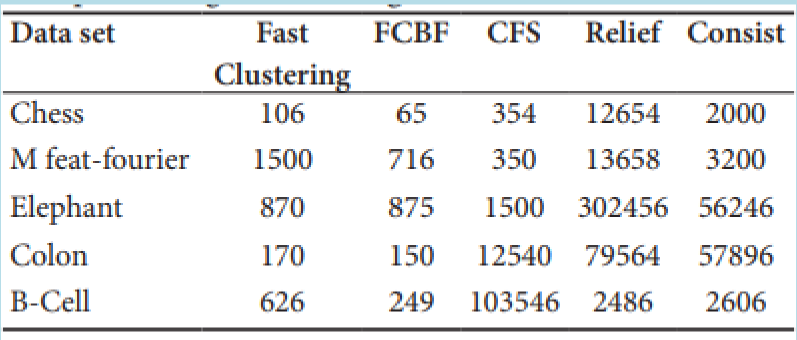
Dr. D. Veeraiah

Associate Professor

"Feature Sub Selection over High Dimensional Data Based on Classification Models"

Abstract

The main objective of this paper achieves feature selection in cluster categorical data sets. Although efforts have been made to fix the problem of clustering particular details via group outfits, with the results being competitive to traditional methods, it is noticed that these techniques unfortunately generate a final details partition based on imperfect details. The actual ensemble-information matrix provides only cluster-data point interaction, with many entries being left unknown. While the performance concerns the time required to find a part of functions, the performance is associated with the quality of the part of functions. Centered on these requirements, Fast clusteringbased function selection algorithm (FAST) is suggested and experimentally analyzed in this paper. Findings: The FAST requirements works in two steps. In the starting point, functions are separated into groups by using graph-theoretic clustering methods. Improvement: Table 1. Runtime comparison of six classifications with processing of clustering



Data set	Fast Clustering	FCBF	CFS	Relief	Consist
Chess	106	65	354	12654	2000
M feat-fourier	1500	716	350	13658	3200
Elephant	870	875	1500	302456	56246
Colon	170	150	12540	79564	57896
B-Cell	626	249	103546	2486	2606

For micro array data, the amount of selected attributes has been proposed by each of the six techniques mentioned in above sections.FAST performs efficient potential outstanding performance in attribute selection from overall data sets.

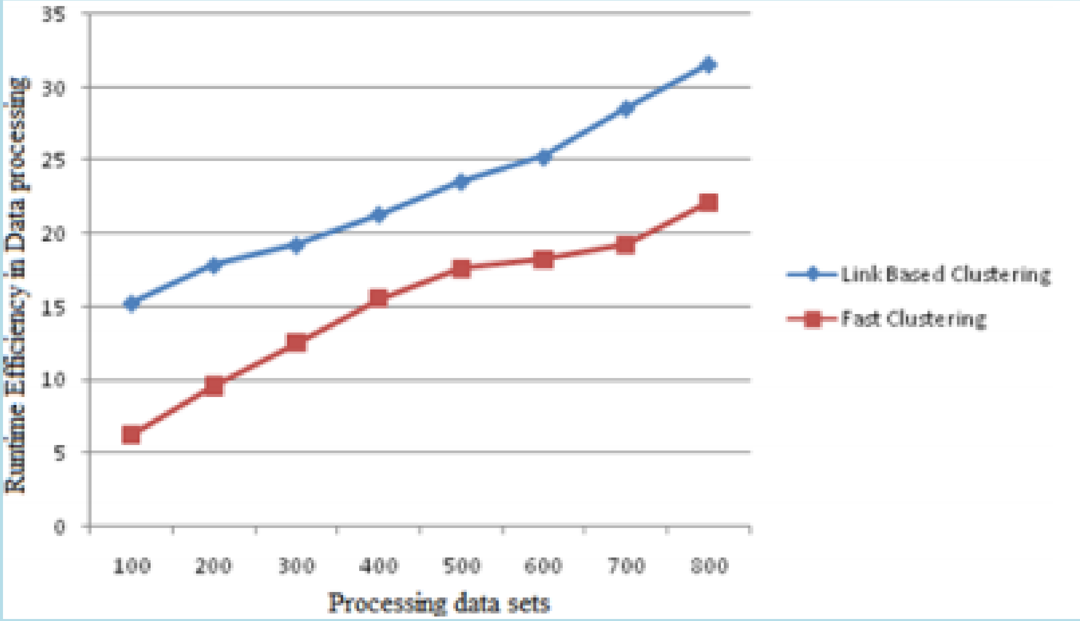


Fig: Performance evaluation with processing data sets in terms of time efficiency

Conclusion

In this paper we present to develop novel feature based sub selection algorithm for high dimensional data. This algorithm involves three main basic components in selection feature from overall data sets. One is irrelevant data removal, constructing minimum spanning tree from relevant nodes from overall data sets. Portioning selected representative features from overall high dimensional data. For this purpose we compare five different well known algorithms FCBF, Relief, CFS, consist performed on publicly available micro array data and text data from different aspects of selected features with runtime execution and classification accuracy with performance evaluation in recent application process. We additionally found that FAST acquires the rank of 1 for smaller scale exhibit information, the rank of 2 for content information, and the rank of 3 for picture information as far as arrangement precision of the four unique sorts of classifiers, and CFS is a decent option. In the meantime, FCBF is a decent option for picture and content information. Besides, Consist, and FOCUS-SF are options for content information.

Ch. V. Narayana

Assoc. Professor

"Handle packet flow and traffic in high speed networks by using Fuzzy logic"

Abstract:

As the increase in usage of computing systems like computers, tablets as well as smart devices there is a large desire for the fast-growing online traffic. Dispensed traffic control frame work has been suggested, in which routers are integrated with smart data rate planners to handle the extreme traffic level. The traffic control prototype is distinctive as more traffic control methods have to determine network guidelines which require link latency, bottleneck bandwidth, packet reduction rate, or the amount of flows to calculate the permitted source delivering level. By the fuzzy logic strategy, QoS (Quality of Service) in communication is guaranteed by good shows of our scheme like maxmin equity, low queuing delay and good robustness to system characteristics. The summary is that the outcomes and evaluations have confirmed the performance and made a provided a new benchmark that our traffic control scheme using fuzzy-logic can accomplish better efficiency than the established prototypes that count definitely on the evaluation of system parameter.

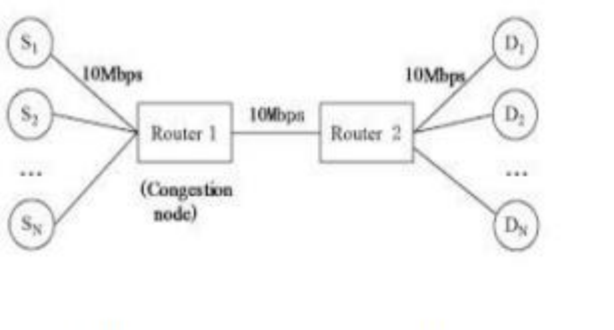


Fig. 1 Basic Configuration of a fuzzy logic system

Protocol (APIRCP)

fuzzy logic traffic controller for controlling traffic in the network system defined in Fig. 1. Called the IntelRate, it is a TISO (Two-Input Single- Output) controller. The aggregate output is y (t) =ui (t - Ti). Under heavy traffic situations, the IntelRate controller would compute an allowed sending rate ui(t) for flow i according to the current IQSize so that q(t) can be stabilized around q0.

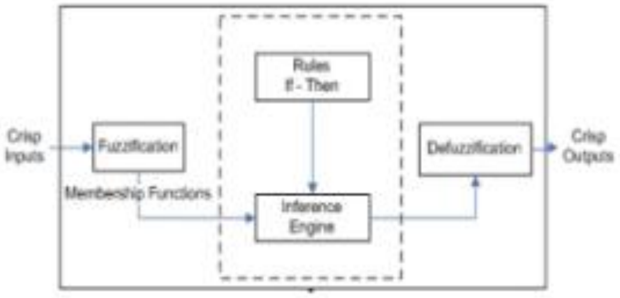


Fig.2 Intelrate Controller System

Conclusion

A creative traffic control scheme, named the Intel Rate controller, has been projected to handle the Internet congestion in order to assure the quality of service for various service programs. The controller is developed by giving consideration to the drawbacks and the benefits of the existing congestion control prototypes. As a dispensed operation in networks, the Intel Rate controller utilizes the instant queue size only to efficiently throttle the source transmitting rate with max-min fairness. The back-pressure algorithm, while being throughput-optimal, is not beneficial in apply for adaptive routing since the delay efficiency can be actually harmful. In the paper, we have provided an algorithm that routes packets on quickest hops when feasible and decouples routing and organizing using a probabilistic splitting algorithm built on the approach of shadow. Probabilistic routing table that depends gradually over time, real packets do not have to examine long routes to enhance throughput; this efficiency is carried out by the shadow "packet..

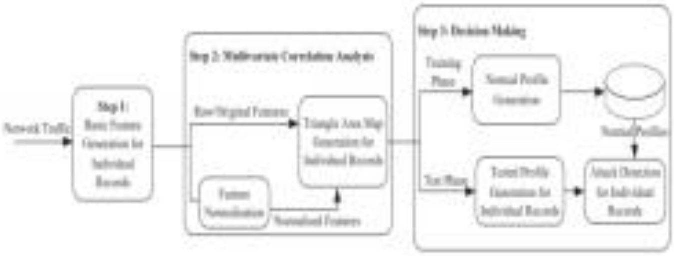
Dr. D. Veeraiah

Associate Professor

"MCA for Detection of DOS Attack"

Abstract

In the networking world, a denial of service (DoS) attack is an incident in which a user is deprived of the services of a resource they would normally expect to have. Intrusion Detection System (IDS) is the tool that is able to detect occurrences of intrusion at host, the network and application in the system. One of the most common network attacks is Denial of Service (DoS) attack. In DoS attack of the computer system an individual host will send huge number of packets to one machine so it make the operating of the network and host slow. In this paper, signature of selected attacks such as Smurf, Ping-of-Death which are based on network flow is considered and MailBomb. The system uses MCA based system for detection of the DoS attack. The proposed system monitors the network path to detect attacks and the results show less false negative error during monitoring of the system. Specially, signature based IDS which use fuzzy decision tree for monitoring network path observes that there are great improvements on speed of detection as well as performance of system in the organization.



Network Traffic
Step 1: Basic Features Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw Original Features
Triangle Area Map Generation for Individual Records
Feature Normalization
Normalized Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Fig 1 :Framework of the proposed denial-of-service attack detection system

The complete detection process consists of three major steps as shown in Fig.1. Initially,In Step 1 basic features are generated from admission network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Step 2 is Multivariate Correlation Analysis(MCA) in which the Triangle Area Map Generation module is applied to enhance the correlations between two distinct features. In Step 3 the anomaly-based detection mechanism is adopted in Decision Making of the data. It facilitates the detection of any DoS attacks without getting any attack related knowledge of the system MCA based detection.

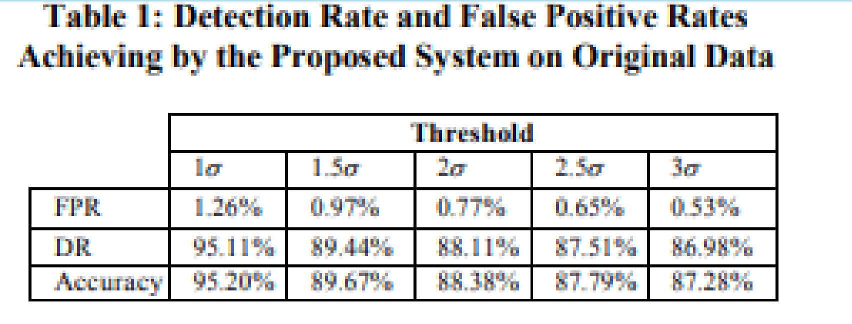
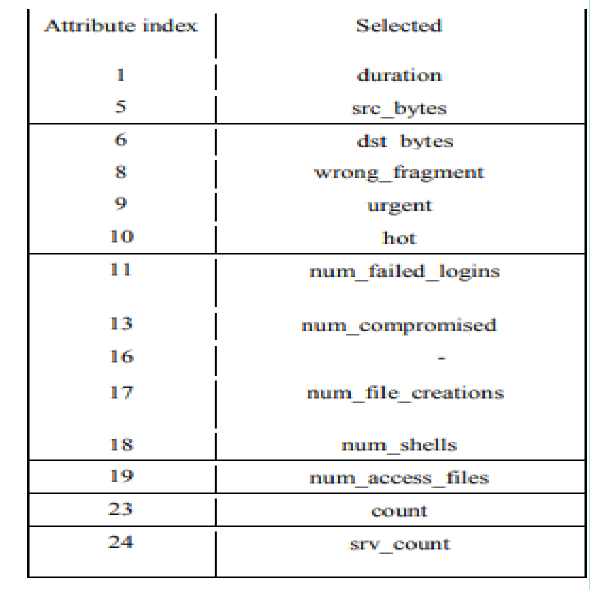


Table 1: Detection Rate and False Positive Rates Achieving by the Proposed System on Original Data

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	1.26%	0.97%	0.77%	0.65%	0.53%
DR	95.11%	89.44%	88.11%	87.51%	86.98%
Accuracy	95.20%	89.67%	88.38%	87.79%	87.28%

Hence, the overall accuracy of the proposed system is computed based on the precision and recall also F-measure which are normally used to estimate the rare class prediction of the data.



Attribute index	Selected
1	duration
5	src_bytes
6	dst bytes
8	wrong_fragment
9	urgent
10	hot
11	num_failed_logins
13	num_compromised
16	-
17	num_file_creations
18	num_shells
19	num_access_files
23	count
24	srv_count

Conclusion

We have developed an anomaly based intrusion detection system for detecting the intrusion within a network. In this fuzzy decision-making module was constructed to generate the system more accurate for attack detection using the fuzzy inference approach. The proposed method is very much useful in detecting various intrusions in computer networks system. Here, the proposed system achieves equal better performance as compared to the two state of the art approaches. In the future work we will further implement our DoS attack detection system with the help of real world data and find more impressive classification techniques to further less severe false positive rate.

Ms. M. Sri Bala

Asst. Professor

"Dynamic Authentication for Efficient Data Storage HMS"

Abstract

Thinking handling has showed up as one of the most significant paradigms in the IT market recently. Since this new handling technology needs clients to trust their valuable information to reasoning providers, there have been enhancing security and comfort issues on shortened details. Several techniques employing attribute-based security (ABE) have been recommended for accessibility management of shortened details in reasoning computing; however, most of them experience from inflexibility in applying complex availability management guidelines. In purchase to identify scalable, flexible, and fine-grained accessibility management of shortened details in reasoning handling, in this papers, we suggest Enhanced Feature based Security by enhancing cipher text-policy attribute-setbased encryption (ASBE) with a requested structure of clients. The recommended plan not only achieves scalability due to its requested structure, but also gets flexibility and fine-grained availability management in assisting material features of ASBE.

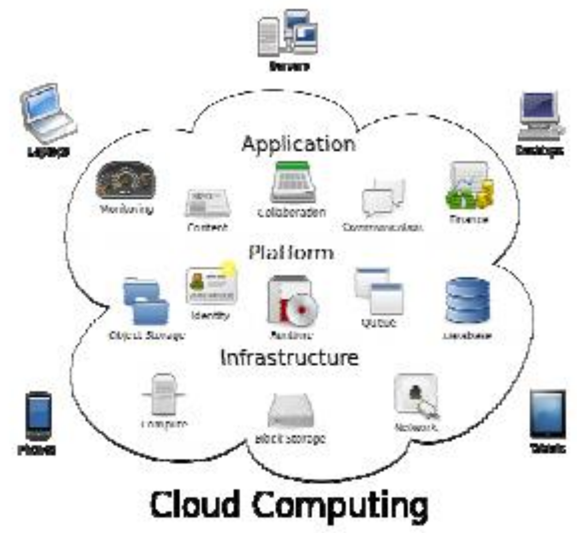


Figure 1: Cloud computing architecture regarding services. [1]

System Setup: When the program is set up, the reliable authority selects a bilinear team and some unique numbers. When keys are generated PK and MKo are produced, there will be several exponentiation functions. So the calculations complexity of Program Installation is O(1).

Top-Level Sector Power Grant: This operation is conducted by the reliable power. The master key of a sector power is of , , (, , ,), MK D D fora E forA i i j i j i i = ∈ ∈ where is the key structure associated with a new domain authority, Ai is the set . Let N be the number of attributes in and M be the number of sets in , then the combination of the procedure MKi consists two exponential values for each attribute.

New User/Domain Power Allow. In this function, a new customer or new sector authority is associated with an attribute set, which is the set of that of the in the domain authority. The primary calculations expense of this operation is randomizing the key.

New information file creation: In this operation, the information owner needs to secure a computer file using the symmetrical key DEK and then encrypt DEK Using EABE. The complexity of encrypting the data file with DEK relies on the size of the data file and the actual symmetrical key security criteria. When re-encrypting details, the details owner just needs two exponentiations for cipher text components associated with the expiration Time so the complexity of the operation is O(1).

Conclusion

In this we present EABE for realizing scalable, versatile, and fine-grained accessibility management in reasoning processing. plan easily has a hierarchical structure of system customers by implementing a delegation algorithm to ASBE.EABE not only facilitates substance attributes due to versatile feature set mixtures, but also accomplishes efficient user cancellation because of several value projects of features. We officially shown the protection of EABE based on the protection of CP-ABE. Lastly, we implemented the suggested plan, and performed comprehensive performance research and assessment, which revealed its efficiency and advantages over current techniques. Further improvement of our suggested work will be developed in multiple customer accessibility management policy with real-time database integration in reasoning processing.

Mr. D. Srinivasa Rao

Sr. Asst. Professor

"Trustee based social authentication: A Novel Approach of authentication"

Abstract

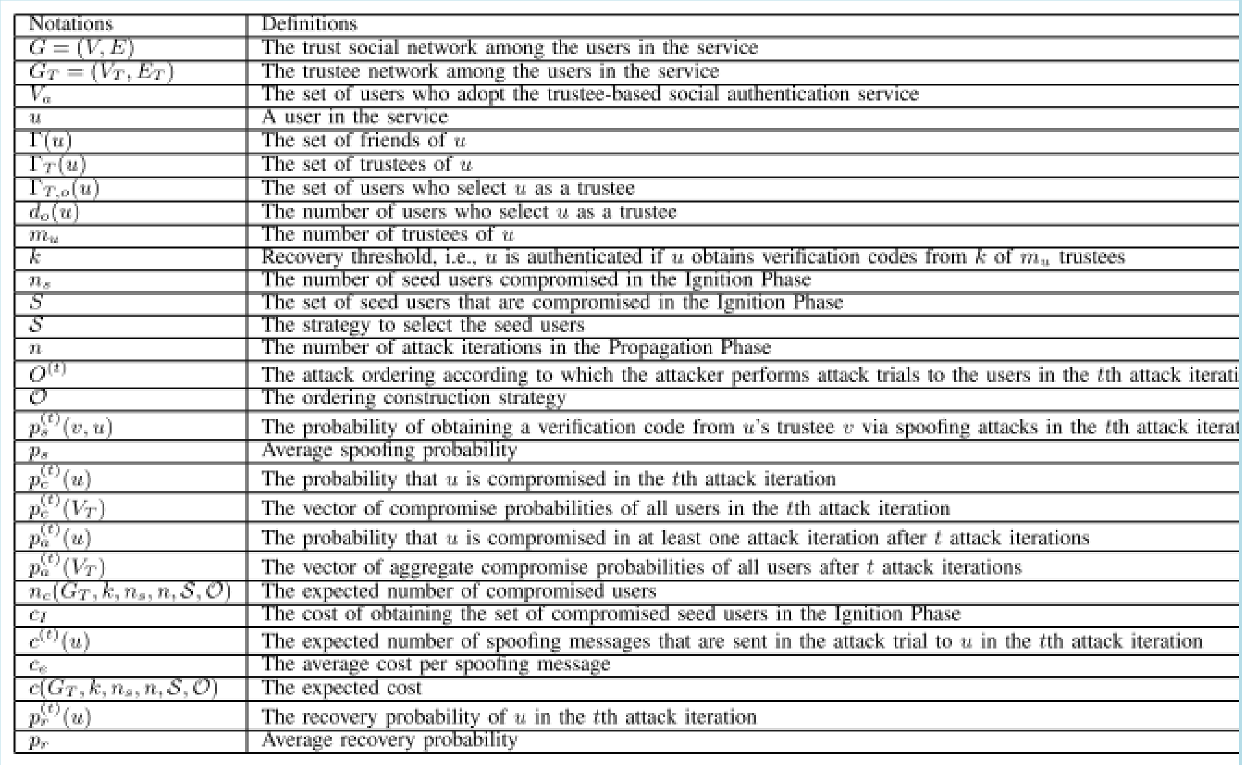
Recently, authenticating users with the help of their friends (i.e., trustee-based social authentication) has been shown to be a promising backup authentication mechanism. A user in this system is associated with a few trustees that were selected from the user's friends. When the user wants to regain access to the account, the service provider sends different verification codes to the user's trustees. The user must obtain at least k (i.e., recovery threshold) verification codes from the trustees before being directed to reset his or her password. Trustee-Based Social Authentications

A trustee-based social authentication includes two phases:

• **Registration Phase.** The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password), and then a few (e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's trustees.

• **Recovery Phase**. When Alice forgets her password or her password was compromised and changed by an attacker, she recovers her account with the help of her trustees in this phase. Specifically, Alice first sends an account recovery request with her username to the service provider which then shows Alice an URL. Alice is required to share this URL with her trustees. Then, her trustees authenticate themselves into the system and retrieve verification codes using the given URL

We assume that attackers know the trustee network in the target service. The reasonableness of this threat model is supported by two evidences. First, attackers can obtain users' usernames. A username is usually a string of letters, digits, and special characters. Moreover, Bonneau et al. showed that a majority (e.g., 96% in their studies) of websites enable attackers to probe if a string is a legitimate username. Thus, strong attackers, who have enough resources (e.g., a botnet) to perform username probings, can obtain all usernames in the target service. Second, Schechter et al. found, via performing user studies, that users cannot remember their own trustees. Therefore, a usable trustee-based social authentication system must remind users of their trustees. Recall that an account recovery request only requires a username. As a result, an attacker could send account recovery requests with the collected usernames to the service provider which reminds the attacker of the trustees of each user.



Notations	Definitions
$G = (V, E)$	The trust social network among the users in the service
$G_T = (V_T, E_T)$	The trustee network among the users in the service
V_a	The set of users who adopt the trustee-based social authentication service
u	A user in the service
$\Gamma(u)$	The set of friends of u
$\Gamma_T(u)$	The set of trustees of u
$\Gamma_{T,o}(u)$	The set of users who select u as a trustee
$d_o(u)$	The number of users who select u as a trustee
m_u	The number of trustees of u
k	Recovery threshold, i.e., u is authenticated if u obtains verification codes from k of m_u trustees
n_s	The number of seed users compromised in the Ignition Phase
S	The set of seed users that are compromised in the Ignition Phase
$\mathcal{S}$	The strategy to select the seed users
n	The number of attack iterations in the Propagation Phase
$O^{(t)}$	The attack ordering according to which the attacker performs attack trials to the users in the tth attack iterati
$\mathcal{O}$	The ordering construction strategy
$p_s^{(t)}(v, u)$	The probability of obtaining a verification code from u's trustee v via spoofing attacks in the tth attack iterat
p_s	Average spoofing probability
$p_c^{(t)}(u)$	The probability that u is compromised in the tth attack iteration
$p_c^{(t)}(V_T)$	The vector of compromise probabilities of all users in the tth attack iteration
$p_a^{(t)}(u)$	The probability that u is compromised in at least one attack iteration after t attack iterations
$p_a^{(t)}(V_T)$	The vector of aggregate compromise probabilities of all users after t attack iterations
$n_c(G_T, k, n_s, n, \mathcal{S}, \mathcal{O})$	The expected number of compromised users
c_I	The cost of obtaining the set of compromised seed users in the Ignition Phase
$c^{(t)}(u)$	The expected number of spoofing messages that are sent in the attack trial to u in the tth attack iteration
c_e	The average cost per spoofing message
$c(G_T, k, n_s, n, \mathcal{S}, \mathcal{O})$	The expected cost
$p_r^{(t)}(u)$	The recovery probability of u in the tth attack iteration
p_r	Average recovery probability

Conclusion

In this paper, we provide the first systematic study about the security of trustee-based social authentications. First, we introduce forest fire attacks. In these attacks, an attacker first obtains a small number of compromised seed users and then iteratively attacks the rest of users according to a priority ordering of them. Second, we construct a probabilistic model to formalize the threats of forest fire attacks and their costs for attackers. Third, we introduce a few strategies to select seed users and construct priority orderings, and we discuss various defense strategies. Fourth, via extensive evaluations using three real-world social network datasets, we find that forest fire attack is a potential big threat.

Ms. K. Naga Prasanthi

Asst.Professor

"FILTER WALL: A System To Filter Unwanted Messages"

Abstract

Internet becomes more and more popular in the day to day activities of user's. In recent years use of online social networks (OSN) also increased rapidly. The users can communicate and share their views, ideas and content through online social networking (OSN). Several types of content like image, text, audio, video etc can be shared between the users. The main drawback of these Online Social Networking (OSN) services is the lack of privacy for the user's own private space. The users can not have ability to direct control to prevent the undesired messages posted on their own private walls. There are only the unwanted messages will be blocked not the user. To avoid this issue, BL (Black List) mechanism is used in this paper, which avoids undesired creators messages.

As far as the learning model has concerned, we confirm in the current paper the use of neural learning which is today recognized as one of the more efficient solutions in text classification. In particular, we base the overall short text classifying strategy on Radial Basis Function Networks (RBFN) for their proven capabilities in acting as soft classifiers, in managing unwanted data and intrinsically vague classes. We insert the neural model within a hierarchical 2 level classification strategy. In the first level, the RBFN categorizes short messages as Neutral and Non-neutral. In the 2nd stage, Non-neutral messages are classified producing

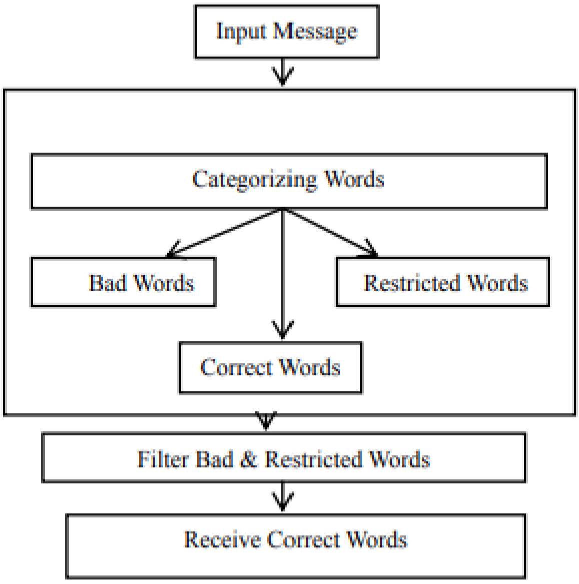


Fig.1. Filtering Process

Conclusion

In this paper, a system in preventing the indecent messages from the Social Networking site walls has been presented. The Usage of Machine Learning system has given higher results to the system to trace the messages and the users to distinguish between the good & bad messages and the authorized & unauthorized users in the Social Networking User Profiles. Thus the Machine Learning system Technique plays an important role in this paper in order to generate the blacklist of the bad words and the users which are unauthorized. The user has to update his privacy setting in his account in order to add this method in preventing the vulgarity in his public profile. In this context, a statistical analysis has been conducted to provide the usage of the good & bad words by the persons in the sites. Overall, the obscenity of the users has been prevented.

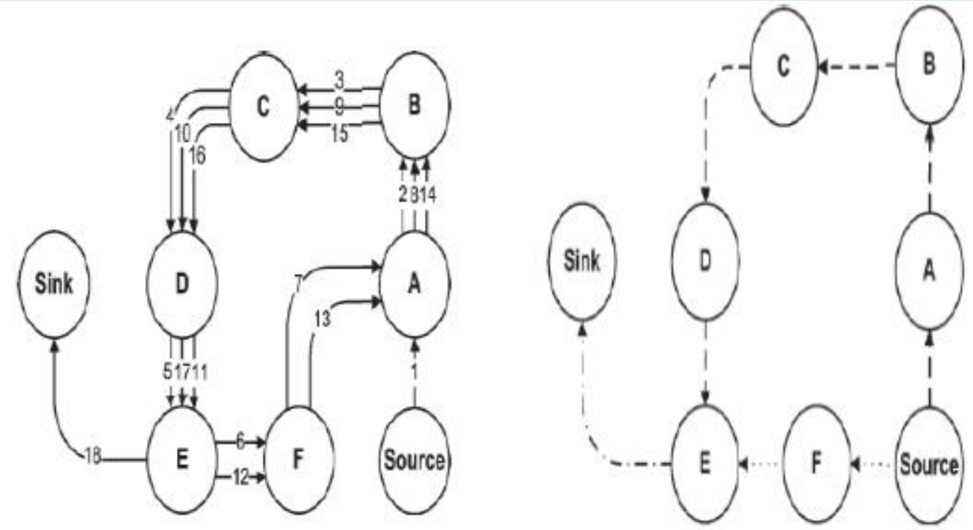
Mr. G Nageswara Rao

Associate Professor

"Secure forwarding of packets from Vampire attacks in wireless adhoc sensor networks"

Abstract

Wireless Ad-hoc Sensor Network is an emerging platform in the field of remote sensing, data collection, analysis, rectification of the problem and research in various studies. The objective of this paper is to examine resource depletion attacks at the routing protocol layer, which attempts to permanently disable network nodes by quickly draining their battery power. This type of attack is called as vampire attack. These attacks are not specific to any protocol, but rather rely on the properties of many popular classes of routing protocols. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N is the number of network nodes. Methods to detect and secure data packets from vampires during the packet forwarding phase is discussed.



(a) An honest route would exit the loop immediately from node E to Sink, but a malicious packet makes its way around the loop twice more before exiting.

(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

Figure 1: Attacks on source routing (a) carousel attack (b) stretch attack

Classification

Denial of service is an attack, where a victim can use 10 minutes of the CPU time to transmit a data packet, but whereas an honest node uses 1 minute of its CPU time to transmit the same data packet. In multihop routing network: a source composes the shortest path and transmits the data packet to the next hop, which transmits it further, until the destination is reached; consuming resources not only at the source node but also at every node the packet moves through. Vampire attack can be defined as a voluntary action of composing and transmitting a malicious message that chooses the longest path which consumes more energy of the network than if an honest node transmits a message of identical size to the same destination.

The strength of an attack can be measured by the ratio of network energy used in the honest case to the energy used in the malicious case. Brief mentions of this attack can be found in other literature, but no intuition for defence or any evaluation is provided. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. However, Vampires will increase energy usage even in minimal-energy routing scenarios. Attackers will produce packets which traverse more hops than necessary, so even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires.

The carousel attack can be prevented entirely by having, forwarding nodes to check the source routes for loops. When a loop is detected, it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). Prevention of data packets from entering into a malicious node is left for future work.

Internships In Academic Year

Name of the Organisation and Place	No.of Students
Anode Info.Tech, Hyderabad	22
BSNL, Vijayawada	1
CITD,MCME, Hyderabad	3
Cyient Ltd, Hyderabad	1
Devmen-IT, Hyderabad	24
Iseef Technologies, Hyderabad	19
Logic Matter, Hyderabad	1
Q-Space, Hyderabad	8
MSMe, Vijayawada	1
Sell.Global Info, vijayawada	14
Satya Tech, Hyderabad	7
NSIC, Hyderabad	3
WebTech.Lab, Hyderabad	10
Y-not SS, vijayawada	2
Vision Tech, vijayawada	1
Naresh.Tech, Hyderabad	1
SNR Investment, Hyderabad	1
Tekcrux pvt Limited, Hyderabad	15
Vision Krest, Hyderabad	1
WebTech.Lab, Hyderabad	7
Web Cognize, Hyderabad	1
Total	**143**

Placement Summary:

S.No	Academic Year	No Of Students Placed	Max Package (In Lakhs)
1	2015-16	84	3.5

Higher Education Details:

Sno	Academic Year	No Of Students
1	2015-16	26

Placement Details:

S.NO	Name of the Company	No of students selected	ANNUAL SALARY (Lakhs)
1	TCS	33	3.18
2	POLARIS	05	3.5
3	FSS	03	2.5
4	VEE TECH	04	2.2
5	MAHAVEER GROUP	08	1.4
6	SUTHERLAND	04	2.4
7	MIRACLE SOFTWARE	06	1.4
8	KNOAH SOLUTIONS	03	2.0
9	TECH MINDS	03	1.6
10	RPOHIRE	04	1.2
11	HCL TECHNOLOGIES	03	2.0
12	EFFTRONICS	01	2.2
13	AMAZON	01	1.2
14	SYNTEL	04	2.0
15	IBM	01	3.0
16	OSMOSYS TECH	01	3.0

SAHELI Club Events:

- An awareness program on "A Community Awakening Caravan To Counter Trafficking" was conducted at LBRCE on 29-02-2016.
- Seminar on "Youth-The Future Of India" organized on 22nd December 2015.

GIRLS BCC ENROLLED LIST

Sr.No	RGTL NO	NAME OF THE CADET
1	APSW/2015/372552	Gavirineni Baby Sindhuja
2	APSW/2015/372553	Konduru Rupa Mounika
3	APSW/2015/372554	Meduri Prabhatha
4	APSW/2015/372555	Veluguleti C N D Sindhusa
5	APSW/2015/372556	Ganagaraju Sudha Madhuri
6	APSW/2015/372557	Chilla Bhuvaneshwari
7	APSW/2015/372558	Parvataneni Geethika
8	APSW/2015/372559	Karedla Poojitha
9	APSW/2015/372560	Bommadevara Monica Bhavani
10	APSW/2015/372561	Vennapusa Sravanthi
11	APSW/2015/372562	Challa Jerusa Esther Rani
12	APSW/2015/372563	Kiranmai Medisetti
13	APSW/2015/372564	Bi Bi Ayeesha
14	APSW/2015/372565	Shaik Rubeena
15	APSW/2015/372566	Mohammad Karishma
16	APSW/2015/372567	B N S D Kameswari
17	APSW/2015/372568	Valluru Prathyusha

Editorial Board

Acknowledgements

At the end, we would like to extend our sincere gratitude to our management for their constant support. Also we would like to thank our Director, Dr. E. V. Prasad and Mentor Dean, Dr. R. Chandrashekaram for their encouragement. We would also like to thank our HOD Dr. N. Ravi Shankar for the innovative ideas for the additions made to our magazine, and Faculty for shaping the TECH-TALK. Also our gratitude to our fellow members of the editorial board and department for their support to the TECH-TALK. Lastly we would like to thank all the faculty members, students and all stakeholders for their valuable inputs.

-The Editorial Team
TECH-TALK

LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING
(AUTONOMOUS)
Approved by AICTE, NEW DELHI, Affiliated to JNTUK, Kakinada
Accredited by NAAC (A) UGC, NBA Accredited, ISO 9001:2008
Certified Institution
MYLAVARAM – 521 230, Krishna Dist., A. P. INDIA.
Tel: 08659-222933, 934, 94401 39918 Fax: 08659-222931

TECH-TALK

Biannual Magazine

> “All of us do not have equal talent. But, all of us have an equal oppurtunity to develop our talents”

COMPUTER SCIENCE
ENGINEERING