IPHV7I10011X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

An Offensive Alert Based Novel Algorithm Of A Forced Entry Scheme In Wireless Adhoc Network

[1]Priyanka Bullah, [2]Arif Mohammad Abdul
Dept of CSE
GITAM University,Hyderabad

Abstract-Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. One threat to timely data delivery in a public network such as the internet is denial-of-service (DoS) attacks: these attacks overwhelm the processing or link capacity of the target site (or routers that are topologically close) by saturating it (them) with bogus packets. Such attacks can seriously disrupt legitimate communications at minimal cost and danger to the attacker, as has been demonstrated in the recent years. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. New intrusion types, of which detection systems are unaware, are the most difficult to detect. Current signature based methods and learning algorithms which rely on labeled data to train, generally cannot detect these new intrusions. In addition, labeled training data in order to train misuse and anomaly detection systems is typically very expensive. We present a new type of clustering-based intrusion detection algorithm, unsupervised anomaly detection, which trains on unlabeled data in order to detect new intrusions. In our system, no manually or otherwise classified data is necessary for training.

General Terms- *Clustering-based intrusion detection algorithm ,Distributed denial of attack, unsupervised anomaly detection, intrusion detection system, security, algorithm*

Keywords - *Classification, fuzzy clustering, intrusion detection, cyber attack, Wireless mobile ad-hoc network, DDoS attack.*

I. INTRODUCTION

Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self routing capability nature, there are many weaknesses in its security. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection [1] and

anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS[2] is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

II. RELATED WORK

The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV & DSR. Wei-Shen Lai et al [3] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [4] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique. Giriraj Chauhan and Sukumar Nandi [5] proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. Xiapu Luo et al [6] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Xiaoxin Wu et al [7] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification Ping. S.A.Arunmozhi and Y.Venkataramani [8] proposed a defense scheme for DDoS attack in which they use MAC layer information like frequency of RTD/CTS packet, sensing a busy channel and number of RTS/DATA retransmission. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [9] proposed DDoS flooding attack detection through a step-by-step.

With the increased usage of computer networks, security becomes a critical issue. A network intrusion by malicious or unauthorized users can cause severe disruption to networks. Therefore the development of a robust and reliable network intrusion detection system (IDS) is increasingly important. Traditionally, signature based automatic detection methods have been widely used in intrusion detection systems. When an attack is discovered, the associated traffic pattern is recorded and coded as a signature by human experts, and then used to detect malicious traffic. However, signature based methods suffer from their inability to detect new types of attack. Furthermore the database of the signatures is growing as new types of attack are being detected, which may affect the efficiency of the detection. Other methods have been proposed using machine learning algorithms to train on labeled network data, i.e., with instances reclassified as being an attack or not (Lee & Stolfo 1998). These methods can be classified into two categories: misuse detection and anomaly detection. In the misuse detection approach, the machine learning algorithm is trained over the set of labeled data and automatically builds detection models. Thus, the detection models are similar to the signatures described before. Nonetheless these detection

methods have the same weakness as the signature based methods in that they are vulnerable against new types of attack.

In contrast, anomaly detection approaches build models of normal data and then attempt to detect deviations from the normal model in observed data. Consequently these algorithms can detect new types of intrusions because these new intrusions, by assumption, will deviate from normal network usage (Javitz & Vadles 1993, Denning 1987). Nevertheless these algorithms require a set of purely normal data from which they train their model. If the training data contains traces of intrusions, the algorithm may not detect future instances of these attack because it will assume that they are normal. In most circumstances, labeled data or purely normal data is not readily available since it is time consuming and expensive to manually classify it. Purely normal data is also very hard to obtain in practice, since it is very hard to guarantee that there are no intrusions when we are collecting network traffic. To address these problems, we used a new type of intrusion detection algorithm called unsupervised anomaly detection. It makes two assumptions about the data.

Assumption 1:

The majority of the network connections are normal traffic. Only X% of tra_c are malicious.(Portnoy, Eskin & Stolfo 2001)

Assumption 2:

The attack traffic is statistically different from normal traffic. (Javitz & Vadles 1993, Denning 1987).The algorithm takes as input a set of unlabeled data and attempts to _nd intrusions buried within the data. After these intrusions are detected, we can train a misuse detection algorithm or a traditional anomaly detection algorithm using the data. If any of the assumptions fail, the performance of the algorithm will deteriorate. For example, it will have difficulties in detecting a bandwidth DoS attack. The reason is that often under such attacks there are so many instances of the intrusion that it occurs in a similar number to normal instances. We took a similar approach to that presented in (Oldmeadow, Ravinutala & Leckie 2004) and (Eskin, Arnold, Prerau, Portnoy & Stolfo 2002) to the problem, and employed a clustering method for the unsupervised anomaly detection. In our approach we chose a clustering method that is designed for dealing with high dimensional data in large data sets. We evaluated our algorithm over real network data. Both the training and testing was done using the KDD Cup 1999 data (KDD 1999), which is a very popular and widely used intrusion attack data set. Our results show that the accuracy of our algorithm approaches that of the previous works. Furthermore, the computational complexity of the algorithm makes this approach promising. Finally, we are able to infer from our results some of the requirements of a good intrusion detection system. The paper is structured as follows. In Section 2, we give a general survey of the field of anomaly detection in network intrusion detection. In Section 3, we describe our clustering algorithm fpMAFIA in detail and illustrate the algorithm with a running example. We also analyze the average case and worst case complexity of our algorithm. In Section 4, we describe the details of our experiment and present the results graphically. In Section 5, we discuss the results and its possible implications. In Section 6, we suggest some possible future directions of the investigation.

III.UNSUPERVISED ANOMALY DETECTION

Anomaly detection is a critical issue in Mobile ad hoc Network Intrusion Detection Systems (MANETIDSs). Most anomaly based MANETIDSs employ supervised algorithms, whose performances highly depend on attack-free training data. However, this kind of training data is difficult to obtain in real world network environment. Moreover, with changing network environment or services, patterns of normal traffic will be changed. This leads to high false positive rate of supervised MANNETIDSs. Unsupervised outlier detection can overcome the drawbacks of supervised anomaly detection. Therefore, we apply one of the efficient data mining algorithms called random forests algorithm in anomaly based MANETIDSs. Without attack-free training data, random forests algorithm can detect outliers in

datasets of network traffic. In this paper, we discuss our framework of anomaly based network intrusion detection. In the framework, patterns of network services are built by random forests algorithm over traffic data. Intrusions are detected by determining outliers related to the built patterns. We present the modification on the outlier detection algorithm of random forests. We also report our experimental results over the KDD'99 dataset. The results show that the proposed approach is comparable to previously reported unsupervised anomaly detection approaches evaluated over the KDD' 99 dataset.

Applying unsupervised anomaly detection in network intrusion detection is a new research area that have already drawn interest in the academic community. Eskin, et al. (Eskin et al. 2002) investigated the effectiveness of three algorithms in intrusion detection: the fixed-width clustering algorithm, an optimized version of the k-nearest neighbor algorithm, and the one class support vector machine algorithm. Old meadow, et al. (Old meadow et al. 2004) carried out further research based on the clustering method in (Eskin et al. 2002) and showed improvements in accuracy when the clusters are adaptive to changing traffic patterns. A different approach using a quarter sphere support vector machine is proposed in (Laskov, Schafer & Kotenko 2004), with moderate success. In (Eskin 2000), a mixture model for explaining the presence of anomalies is presented, and machine learning techniques are used to estimate the probability distributions of the mixture to detect anomalies. In (Zanero & Savaresi 2004), a novel two-tier IDS is proposed. The first tier uses unsupervised clustering to classify the packets and compresses the information within the payload, and the second tier used an anomaly detection algorithm and the information from the first tier for intrusion detection. Lane and Brodley (Lane & Brodley 1997) evaluated unlabeled data by looking at user profiles and comparing the activity during an intrusion to the activity during normal use. Supervised anomaly detection in network intrusion detection, which uses purely normal instances as training data, has been studied extensively in the academic community. A comprehensive survey of various techniques is given in (Lazarevic, Ertoz, Kumar, Ozgur & Srivastava 2003). An approach for modeling normal traffic using self-organising maps is presented in (Gonzalez & Dasgupta 2002), while another one uses principal component classifiers to obtain the model (Shyu, Chen, Sarinnapakorn & Chang 2003). One approach uses graphs for modeling the normal data and detect the irregularities in the graph for anomalies (Noble & Cook 2003). Another approach uses the normal data to generate abnormal data and uses it as input for a classification algorithm (Gonzalez & Dasgupta 2003).

Clustering:

Clustering is a well known and studied problem. There exist a large number of clustering algorithms in the literature. These methods can be categorized as: partitioning methods, hierarchical methods, density based methods and grid-based methods. We shall concentrate on algorithms that closely related to our investigation.

IV.CLUSTER FORMATION

In this paper, we have proposed an algorithm where intrusion detection has been done in a cluster based manner to take care of the ddos attacks. The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a wormhole attack. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of view, this will also reduce the risk of a cluster head being compromised. The entire network is divided in clusters as in figure 2. The clusters may be overlapped or disjoint. Each cluster has its own cluster head and a number of nodes designated as member nodes. Member nodes pass on the information only to the cluster head. The cluster-head is responsible for passing on the aggregate information to all its members. The cluster head is elected dynamically and maintains the routing information. GN is the guard node, used for monitoring the malicious activity. The main purpose of the guard node is to guard the cluster from possible attacks. The guard node

IPHV7I10011X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

has the power to monitor the activity of any node within the cluster. The guard node reports to the cluster head ofthe respective layer in case a malicious activity is detected. A cluster head in the inner layer (CH1,i) detects a malicious activity and informs the cluster head CH2 of the outer layer to take appropriate action. It's the duty of (CH1,i) to check the number of false routes generated by any node. The cluster head CH2 of outer layer takes upon itself the responsibility of informing all nodes of the inner layer about the malicious node.

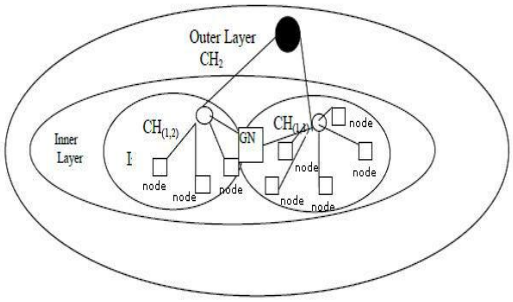

Figure 2 - The Layered structure

Attack in clustering:

According to the impact of the malicious nodes in clustering, we divide the attack into direct clustering attack and indirect clustering attack. In the direct clustering attack, the malicious nodes discourage the cluster head election procedure, which will make the network difficult to build the clusters. Moreover, it is unable to establish the routing in clusters. Thus, this kind of attack can further destroy the communication in the networks. Flooding [5] and rushing [6]are the typical direct clustering attack. To complete the indirect clustering attack successfully, firstly malicious nodes should be chosen as cluster heads with the benefit of fake metrics (e.g., degree and mobility) in cluster head election procedure. After that, these malicious cluster heads can carry out diverse attacks in the routing. Compared with the direct one, the indirect clustering attack is more difficult to be detected. Wormhole attack [7] is an example of this kind attack. In the clustering, the attackers are successful to be the gateway nodes, and then they attack the network as the role of the backbone nodes. Figure 1 shows the wormhole attack in the process of clustering. Node A and B are the malicious nodes in the wormhole attack, and they are respectively in two widely separated clusters C and D. They associate with each other and send the cluster information to each other through the wormhole tunnel they build. And then, the malicious node can cheat the cluster head and be elected as the gateway node. That is, the wormhole attackers build a backbone link C-A-B-D. They can carry out many kinds of attacks in this link, such as black hole attack and resource consuming attack.

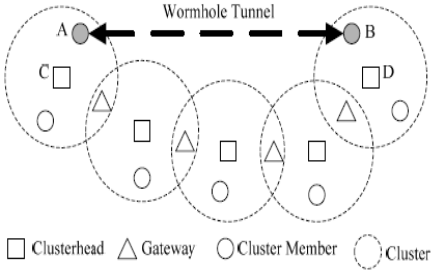

Fig. 1: Wormhole attack in the process of clustering

Partitioning Methods

Given a database of n objects, a partitioning method constructs k partitions of data where each partition represents a cluster. One partitioning method that is of interest to our study is the _xed width clustering algorithm. It is one of the algorithms used in the studies by Stolfo, et al. (Eskin et al. 2002) and Oldmeadow, et al. (Oldmeadow et al. 2004) which we compare our results against. The main advantage of the fixed width algorithm is that it scales linearly with the number of objects in the data set and the number of attributes of the objects. Nevertheless the quality of the clusters is sensitive to the definition of the width of cluster w. Often the user needs several repetitions of the algorithm to choose the best value of w in any particular application.

Density-based Methods:

Density-based methods are based on a simple assumption: clusters are dense regions in the data space that are separated by regions of lower density. Their general idea is to continue growing the given cluster as long as the density in the neighborhood exceeds some threshold. In other words, for each data point within a given cluster, the neighborhood of a given radius has to contain at least a minimum number of points. These methods are good at filtering out outliers and

discovering clusters of arbitrary shapes. Some examples of density-based methods are DBSCAN (Ester, Kriegel, Sander & Xu 1996) and OPTICS (Ankerst, Breunig, Kriegel & Sander 1999).

Grid-based Methods:

Grid-based methods divide the object space into a infinite number of cells that form a grid structure. All of the clustering operations are performed on the grid structure. The main advantage of this approach is its fast processing time, which is typically dependent mainly on the number of cells in each dimension in the quantized space. Some examples of grid-based methods are STING (Wang, Yang & Muntz 1997), Wave Cluster (Sheikholeslami, Chatterjee & Zhang 1998), CLIQUE (Agrawal, Gehrke, Gunopulos & Raghavan 1998) and pMAFIA (Nagesh, Goil & Choudhary 2000). Our work builds upon the CLIQUE and pMAFIA algorithms. CLIQUE (CLustering In QUEst) (Agrawal et al. 1998) is a hybrid clustering method that combines the idea of both grid-based and density-based approaches. CLIQUE first partitions the n-dimensional data space into non-overlapping rectangular units. It attempts to discover the overall distribution patterns of the data set by identifying the sparse and dense units in the space. The identification of the candidate search space is based on the following monotonicity principle: if a k-dimensional unit is dense, then so are its projections in (k 1) dimensional space. pMAFIA (Nagesh et al. 2000) is an optimized and improved version of CLIQUE. There are two main differences between them. First, pMAFIA used the adaptive grid algorithm to reduce the total number of potential dense units by merging small 1-dimensional partitions that have similar densities. Second, it parallelized the operation of the generation and population of the candidate dense units using a computer cluster. However, they both scale exponentially to the dimension of the cluster of the highest dimension in the data set.

V.ALGORITHMS

Reputation Evaluation:

In our reputation evaluation mechanism, the reputation is evaluated by combining the experience of the node in the routing process. We can master the security situation of nodes through the reputation value to choose the nodes with higher value, thus ensuring communication reliability. The reputation of the node is evaluated through the capability of the node in dealing with packets in the routing process. In ad hoc networks, the behaviors of the node involve processing routing control messages and data packets in the routing. Attack measures of these two kinds of packets include forging, deleting, and tampering. Considering these, attack actions can be divided into selfish and malicious attacks. In a selfish attack, the nodes may drop the data packets entirely or proportionally to save energy. In a malicious attack, the nodes may transact the routing control messages abnormally, which can result in increasing resource consumption and destroying the routing process. Therefore, we classify the reputation of the node into Selfish Reputation (SR) and Malicious Reputation (MR), which denote the different aspects of nodes in the routing process. The manifestation of a selfish attack is that the attacker drops the data packets in proportion, and its damage potential changes from quantity to quality, which can indicate the risk intensity through the accumulation of dropped packets. We assume that the activity of each node is random (i.e., the moving velocity of the node is uncertain.). Moreover, we evaluate the BR of each node by period and we assume that the numbers of positive and negative samples are S and F, respectively. Bayesian theory can be used to evaluate the quality of service. We have deduced the reputation value in our previous work [8].The selfish reputation value is written as

$$R_f = \frac{S+1}{S+F+2} \qquad (1)$$

Compared with selfish attack, a malicious attack is sudden, and if the condition the attack needs to function is satisfied, it can destroy the network to a certain extent. Therefore, we set different values for the two kinds of reputation evaluation. In SR, we set the value to 1. In MR, the value of a will change with the degree of attack; that is, the more serious the attack, the higher the values are. The reputation value can be calculated as follows.

IPHV7I10011X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

$$R = \omega_f R_f + \omega_m R_m \quad (\omega_f + \omega_M = 1) \qquad (2)$$

Clustering Algorithm:

In this paper, we propose a secure clustering algorithm SCAR, which takes into account a combined weight metric, including the reputation value, the node' degree [9] and the relative mobility [10]. The weight is calculated as follow.

(1) Cluster head election

In the initial of establishing cluster, the nodes are assigned as the role (i.e., cluster head, gateway and cluster member) in the cluster through the clustering procedure. Each node broadcasts Hello message to its neighbor nodes periodically for connectivity. In our algorithm, the weight information is carried in Hello message. When the node receives its neighbor nodes' Hello messages, it updates the related nodes' reputation value. In addition, the node can update its degree and mobility, according to the number of Hello messages received and the transmission power, respectively. After receiving Hello message in some period, the node gets its initial weight. Then the node sends its weight through the broadcasted Hello message. Compared with other nodes' weight, the node that has the highest weight is elected as cluster head. If the node A receives the cluster head message from its neighbor node B, and node B's reputation value is higher than A's, A will send the message to node B to join in its cluster. If node A hasn't received the cluster head's message during a period, it becomes an isolate cluster head which has no cluster member.

(2) Cluster update

Cluster update includes cluster rebuild and cluster healing. Although the cluster is established, the topology of the network still may change due to the mobility of node, the descending of the energy and other factors. Thus, the node may leave the original cluster, or the node may join in the cluster. The original cluster will not be effective. This is cluster reestablishment. In the cluster healing procedure, we set the related threshold according the node's role, i.e., *T*CH, *T*GW and *T*CM (*T*CH>*T*GW>*T*CM) are the thresholds of cluster head, gateway and cluster member, respectively. When the node's reputation value is higher than its role's reputation threshold, it is suspicious. And then, if this node is cluster head or gateway, search its neighbor's reputation value. If it is higher than this suspicious node's, cancel the suspicious node's role of cluster head, and elect this node as cluster head. Else, keep the suspicious node's role. If the suspicious node is cluster member, put it into the black list and isolate from the network.

V. CONCLUSIONS AND DISCUSSIONS

Traditional security mechanisms have addressed the first two parts of this informal definition of security, but largely ignored the timeliness or service guarantee issue. One threat to timely data delivery in a public network such as the internet is denial-of-service (DoS) attacks: these attacks overwhelm the processing or link capacity of the target site (or routers that are topologically close) by saturating it (them) with bogus packets. Such attacks can seriously disrupt legitimate communications at minimal cost and danger to the attacker, as has been demonstrated in the recent years. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. New intrusion types, of which detection systems are unaware, are the most difficult to detect. Current signature based methods and learning algorithms which rely on labeled data to train, generally cannot detect these new intrusions. In addition, labeled training data in order to train misuse and anomaly detection systems is typically very expensive. We present a new type of clustering-based intrusion detection algorithm, unsupervised anomaly detection, which trains on unlabeled data in order to detect new intrusions. In our system, no manually or otherwise classified data is necessary for training.

IPHV7I10011X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

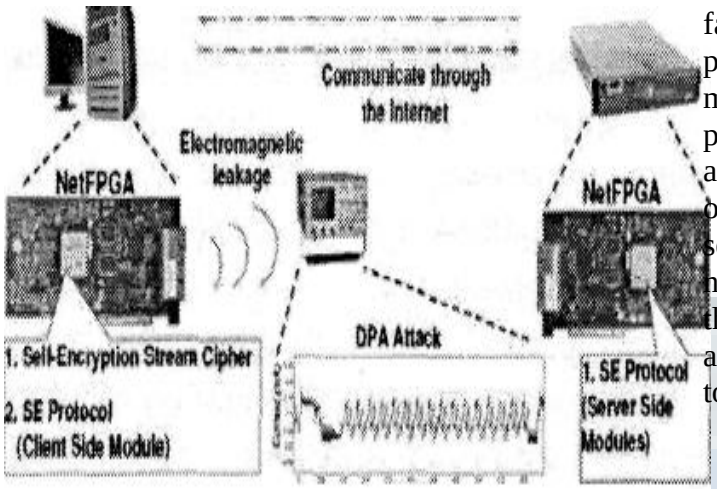

Figure 4. Prototype Implementation & Experiment Platform Construction.

Figure 4 presents the prototype implementation and physical attack study system architecture. At the server side, we plan to implement the SE protocol on a NetFPGA board inserted in a Dell 2950 server. As the mobile device side, we are considering to implement the SE stream cipher scheme and SE protocol on another NetFPGA board inserted in a PC, which is connected to the network through wireless connection.

Devices such as oscillo graph will be used to monitor and record the electromagnetic leakage when the SE stream cipher is being executed to encrypt/decrypt the data. As shown in middle of Fig. 4, an adversary may perform DPA attacks by analyzing the variance of leaking electromagnetic wave. Actually, we expect that our SE stream is not vulnerable to DPA attacks due to the uniqueness of each key stream and a much larger key stream space. However, we are also prepared to improve the implementation if vulnerabilities are observed on the prototype.

Aside from investigating the potential security vulnerability, we will study the performance issues using the prototype in the context of real applications. Considering the resource constraints in the typical mobile devices, the proposed SE stream cipher is hardware-oriented and aims at light-weighted design. We will explore the tradeoffs between the performance and resource utility by the SE system. We have defined a facility (transactions) which clients can use to perform complex updates to distributed data in a manner that maintains consistency in the presence of system crashes and concurrency. Our algorithm for implementing transactions requires only a small amount of communication among servers. This communication is proportional to the number of servers involved in a transaction, rather than the size of the update. We have described the algorithm through a series of abstractions, together with informal correctness arguments.

VI. REFERENCES

[1] J. Al-Muhtadi, D. Mickunas, and R. Campbell, "A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices," *IEEE Wireless Communications*, April 2002.

[2] D. J. Bernstein, "Which eSTREAM ciphers have been broken?" http://www.ecrypt.eu.org/ stream/, submitted 2008-02-21.

[3] A. Biryukov, "Block Ciphers and Stream Ciphers: The State of the Art," *Lecture Notes in Computer Science, in Proceedings of the COSIC Summer course*, 2003.

[4] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," in *Proceedings of Asiacrypt'OO,* no. 1976 in Lecture Notes in Computer Science, pp. 1-13, Springer-Verlag, 2000.

[5] W. Daniel, T. Pintaric, F. Ledermann, S. Dieter, "Towards Massively Multi-User Augmented Reality on Handheld Devices", *International Conference on Pervasive Computing, Munich,* Germany, 2005.

[6] D, E. Denning and D. K. Branstad, "A Taxonomy for Key Escrow Systems," *Communications of the ACM,* Vol. 39, Issue 3, 1996.

[7] eSTREAM, ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream.

. *Notes in Computer Science,* pp. 239-255, edited by W. Fumy, Springer-Verlag, 1997.

[8] T. Good and M. Benaissa, "Hardware performance of eStream phase-Ill stream cipher candidates," *the State of the Art of Stream Ciphers Workshop-* (SASC'08), Lausanne, Switzerland, Feb. 13-14, 2008.

[9] K. Greene, "Securing Cell Phones," *Technology Review,* MIT, Wednesday, Aug. 01, 2007.

[10] J. Hastad and M. Naslund, "Improved analysis of the BMGL keystream generator," in *Proceedings of the Second NESSIE Workshop,* 2001.

[11] Eswaren, K. P. et al. The notions of consistency and predicate locks in a database system. Comm. ACM 19, 11. 624-633, (Nov 1976).

[12] Gifford, D.K. Violet: An experimental decentralized system. Submitted to 7th Symposium on Operating System Principles, 1979.
[13] Gray, J.N. Notes on data base operating systems. In Operating Systems, An Advanced Course, American Elsevier, 1978.

AUTHOR"S PROFILE:

Ms.Priyanka Bullah student in GITAM University, Hyderabad pursuing her M-Tech in dept of CST, and research area in the field of MANET's

Mr.Arif Mohammad Abdul working as an assistant prof. in Dept.of CSE, GITAM university, Hyderabad.He received his M-Tech degree in the 2010 from Sri Indu College Of Engineering & Technology, Hyderabad and received Bachelor of Engineering (B.E) in computer science in 2004 from Maharshi Dayanand University Haryana. Registered PhD in the computer Science in the year 2012 and he is doing research in the area of Trusted Cloud Computing. His Research papers are "Trusted System in Cloud Environment" in the area of Cloud Computing in the year 2013 and "A Novel Approach For Extracting Medical Reports Using Mining Techniques" in the area of Data Mining in 2010.