Inspection of High Risk Containers

Aiman Khan[1], Pallavi N[2]
Department of Computer Science Engineering
[1,2] Atria Institute of Technology

Abstract- *Evaluation of risk containers remain a difficult task and major reason contributing to this difficulty is ambiguous or incomplete information about the containers. This paper deals with three approaches that are mathematical model, similarity model and APRICOIN that would help in inspection and prevention of importation of risk containers.*

Keywords- Inspection, Prevention, Fuzzy Rules, Fuzzy Inference System, APRICOIN

I. INTRODUCTION

Since the introduction of shipping containers in 1960, this has become the standard mode of freight transport. container terminals (CT) assure the liability of the freight transport and therefore must be seen as the cornerstone of the global supply chain. the international community has proposed the Initiative for Safe Containers (ISC) which requires the targeting and inspection of high-risk containers at seaports before shipment. [1] Several technologies can be used to detect a nuclear weapon and a variety of newer technologies are undergoing development. The government needs to identify a testing strategy that specifies which containers to test, how to test them, where to test them (at the overseas port of embarkation, at the domestic port of debarkation, or both), and how many resources (people and equipment) are required to guarantee, with a high probability, that containers are safe to import [2]. The multi- agent aspect of the problem leads us to use a game- theoretic approach. So, this uses a total mathematical model to detect all the aspect and implement according to game theory principles. Next approach would inspect by using statistical model. The concept of fuzzy logic, proposed in 1965 by Zadeh, has been used to manage a kind of probability. To employ this concept, the generalized trapezoidal fuzzy numbers (GTFNs) are most the most popular in practice. A model for a fuzzy-number similarity method between GTFNs has been created, based on the weights associated to each similarity measure [3]. This model uses the cosine coefficient and the Jaccard Index. Third approach is APRICOIN. The precision of the container's risk quantification process is strongly related to two main factors. The first factor is the availability and correctness of a container's descriptive information at their declaration to customs. The second factor is the subjectivity of a container's risk evaluation by customs agents [4] who often rely on their experience in targeting fraudulent containers. The first step of this approach is by mentioned the information of each container and that is given in the form of ECD i.e., Enriched Container Descriptive. Then, the FP- Growth algorithm is used to mine the most occurring items and assign the fuzzy inference rules for the risk factors. Fuzzy inference system uses this score to asses a risk score of the container.

II. THE 11-LAYER SECURITY SYSTEM

The analysis consists of 11 layers of protection. The first three layers attempts to detect the hazard before the container enters into the port for exportation or importation [5]. The first layer is a voluntary self-certification system which recognizes the company that fulfils certain measures as the company eligible to transport.

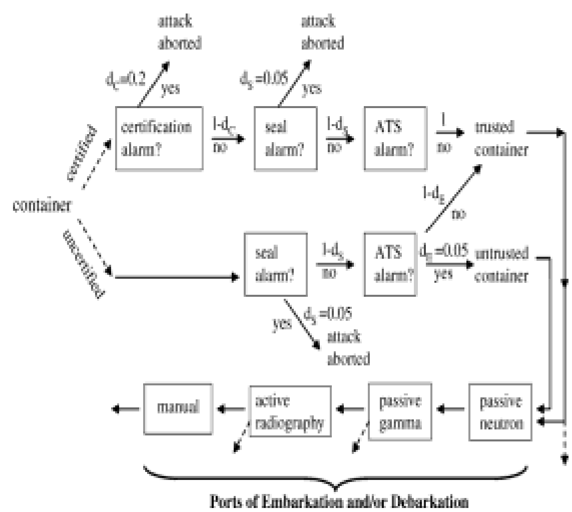

Figure 1 The 11 layers

The second layer is each containers mechanical seal that allows remote verification of serial number but require manual verification to make sure that the seal is intact. This layer sets off an alarm if a terrorist attempts to put a nuclear weapon into the container. The third layer deals with the verification of documents, accompanying container via the U.S. Customs' Automated Targeting System (ATS), that identifies suspicious containers at the port based on their manifest and customs entry document, as well as whether the shipper is self- certified via the C- TPAT Program [6].

The first three security layers do not incorporate any detailed modelling. These layers are included so that we can assess the effectiveness of currently implemented system. All three layers are in technological flux, in that their detection probabilities could increase significantly over the coming years.

The last eight layers involve four layers at each port while two passive tests are performed by an equipment. These two tests measure the emission of gamma rays as they pass by a portal monitor. It is seen that these rays can be veiled by terrorists shielding so, the third layer is gamma radiography which emits gamma rays from one side of the container and measures how many of these rays come out to the other side of the container. This allows to see dense material such as shielding. Final layers is the manual testing where a group of people open up the container and examine its contents. The precise routing of the container through the last stage depends on the testing strategies that are being implied upon it [2].

III. TESTING STRATEGIES

Testing of containers at the location where there are sealed is not considered because of reliable cost of enforcing the security of the containers at that location. The four testing layers are hierarchical where passive tests are easier to monitor, active tests take longer but it detects shielding and manual testing is most expensive but reliable.

[2] All testing strategies are denoted by YZ(a) where Y is the set of containers that might be tested and (Y=A for all and Y=U for untrusted). Z defines where these strategies are applied (Z=D for port of debarkation, D=e for port of embarkation and D=B for both the ports).

Strategy A: Passive (neutron and gamma‐ ray) radiation monitoring of all containers followed by active (gamma radiography) testing of all untrusted containers, of trusted containers failing radiation monitoring, and of a fraction a of trusted containers that pass radiation monitoring.
Strategy U: Trusted containers are not tested. Passive radiation monitoring of all untrusted containers, followed by active testing of untrusted containers failing radiation monitoring, and of a fraction a of untrusted containers that pass radiation monitoring.

If a container fails any of the two tests it goes for subsequent test until the reason of failure is found.

IV. PROPOSED SYSTEM

Risk of a container that is to be transported is calculated as the product of the probability of failure (Pof) and the cost of failure (Cof). To reduce the risk, we can either reduce Pof or/and Cof. In this case Pof is the failure of customs in inspection and Cof is the consequences of failure. The proposed approach was developed to prioritize the risk containers according to their risk scores. This enables the identification and prioritization of high risk containers for thorough inspection. To curate this a three step process was developed [1].

The first step is the container information flow. The first advantage of intelligent container is its ability to collect, store and transmit information during the entire process. It helps to identify the container that has been declared falsely. The second advantage is the quantitative nature of some of the information provided by the intelligent container, which helps in assessing the risk score precisely.

The second step deals with evaluating container's risk and generating a risk score. Frequent pattern mining is used to extract a key criteria that occurred frequently. FP Growth algorithm is used to mine the key ECD criteria. The second step also deals with the risk assessment using fuzzy inference rules system.

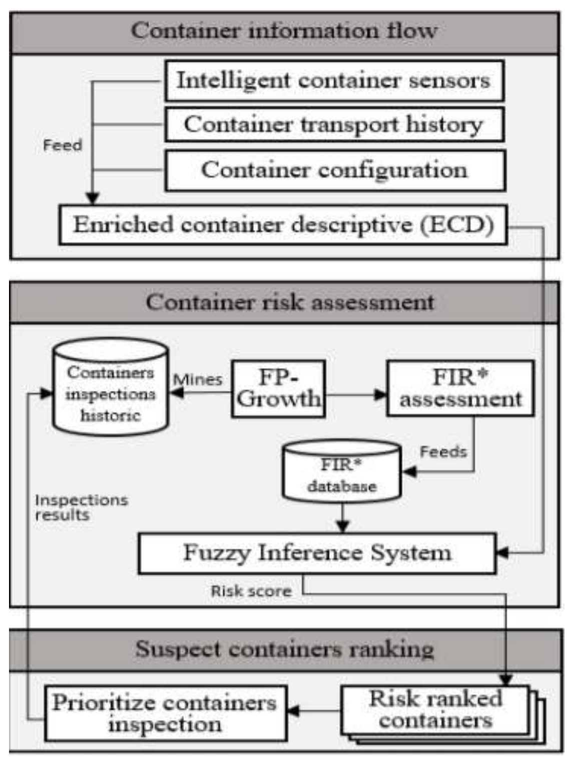

Figure 2 Proposed Approach

V. APRICOIN ALGORITHM

The APRICOIN algorithm describes the main steps followed by FP Growth and fuzzy inference rules system. The algorithm has two inputs: inspection history of the containers and list of containers to be inspected. The first step is to prepare dataset in Boolean form for FP Growth implementation. The Boolean ECDs are stored in database booleanInspectHist.

The second step consists of mining the frequent criteria from inspection history to construct fuzzy inference rules system. This step is repeated each month to adapt fuzzy inference rules for any new emerging key criteria. We call the FP-Growth algorithm to mine frequent criteria from the Boolean inspection history (booleanInspectHist). The mined frequent criteria sets (FCriteriaSets) are then used to asses fuzzy inference rule.

```
    Input: inspectHist //inspections history,
           containersSet //a set of containers
    Output: inspectionPriority //prioritized list of
    containers to be inspected
/*Step1: Prepare inspections dataset
 1. for each ECD from inspectHist do
 2.  booleanECD ← ECDToBoolean(ECD);
 3.  booleanInspectHist.add(booleanECD);
 4. end for
/*Step2: Frequent criteria mining and fuzzy rules
construction
 5. for each month do
 6.  fCriteriaSets ← FPGrowth
       (booleanInspectHist);
 7.    for each set from fCriteriaSets do
 8.      fuzzyRule← assessFuzzyRule(set);
 9.      fuzzyRuleDB.add(fuzzyRule);
 10.   end for
 11. end for
/*Step3: Assess risk score
    for each ECD from containersSet do
 12. quantCriteria ← getQuant(ECD);
 13. FRules← getRules(fuzzyRuleDB);
 14. riskScore ← fuzzyEngine(quantCriteria,
       FRules);
 15. scoresList.add(riskScore);
 16. end for
/*Step4: Containers ranking
 17. rankedList← sortList(scoresList);
 18. inspectionPriority←listTrim(inspectionRate,
     rankedList);
/*Step5: Inspections history feed
 19. High-
     riskContainers←getConcludingInspections();
 20. inspectionsHistory.add(High-riskContainers);
```

Figure 3 APRICOIN Algorithm

The third step is to assess container's risk score by fuzzy inference engine. For each ECD, we use the function getQuant to extract quantitative values of its criteria. The obtained scores are stored in the scores list named scoresList.

The fourth step is sorting the score list then trimming the list using inspection rate as a limit. As a result, we have a list of inspection priority.

The final step consists of feeding the inspections history with the ECDs of the inspected containers with concluding inspection results.

VI. CONCLUSION

The analysis identifies key uncertainties that need to be resolved before a testing strategy can be proposed without any uncertainties. These include the fraction of containers that can be penetrated and/or deciphered by gamma radiography and/or x- ray radiography, the fraction of penetrable containers with a weapon that would be correctly diagnosed by radiography, and the nature of the threat, including the source (uranium vs. plutonium vs. radiological) and the terrorists' shielding capabilities. In this regard, given the difference in detection probability versus cost for the various terrorist decisions, it is imperative that the authority engage in asymmetric packing of objects to ensure robustness of any implemented system.

In APRICOIN approach, the authors developed a prioritizing algorithm (APRICOIN) for the inspection of high-risk containers. The proposed solution exploits the potential of the intelligent container concept to enhance the informative flow through the ECD, and combines frequent pattern mining techniques with a fuzzy system to assess the container's risk score. Inspection prioritization is based on the container's risk score. This assists customs agents in targeting high-risk containers and prioritizing their inspection.

There are still several opportunities for future work. The adjustment of fuzzy inference rules and the accuracy improvement is of keen interest.

REFERENCES

[1] Mohamed Yassine Samiri, Mehdi Najib, Abdelaziz Elfazziki, Mohamed Nezar Abourraja, Dalila Boudebous, And Abdelhadi Bouain, "APRICOIN: An Adaptive Approach for Prioritizing High-Risk Containers Inspections", IEEE, September 18, 2017.

[2] Lawrence M. Wein, Alex H. Wilkins, Manas Baveia, Stephen E. Flynn, "Preventing the Importation of Illicit Nuclear Materials in Shipping Containers", Risk Analysis, An International Journal of the Society of Risk Analysis.

[3] Chen, SM (1996). New methods for subjective mental workload assessment and fuzzy risk analysis. Cybernetics and Systems.

[4] Review of Maritime Transport, UNCTAD, Geneva, Switzerland, 2016.

[5] May, M. M., Wilkening, D., & Putnam, T. L. (2004). Journal of Physical Security.

[6] Stana, R. M. (2004). U.S. General Accounting Office Report GAO- 04- 557T