Detecting Intrusions within RFID Systems through Non-Monotonic Reasoning Cleaning

Author

Darcy, P, Stantic, B, Mitrokotsa, A, Sattar, A

Published

2010

Conference Title

Proceedings of the 2010 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2010

DOI

10.1109/ISSNIP.2010.5706753

Detecting Intrusions within RFID Systems through Non-Monotonic Reasoning Cleaning

Peter Darcy [#1], Bela Stantic [#2], Aikaterini Mitrokotsa [*3], Abdul Sattar [#4]

[#] *Institute for Integrated and Intelligent Systems, Griffith University*
Queensland, Australia
{[1] P.Darcy,[2] B.Stantic,[4] A.Sattar}@griffith.edu.au

[*] *Ecole Polytechnique Fédérale de Lausanne*
Lausanne, Switzerland
[3] Katerina.Mitrokotsa@epfl.ch

***Abstract*—Radio Frequency Identification (RFID) technology uses wireless radio technology to automatically track items spanning various locations with little effort or cost. It is used for various applications such as supply chains and health care. Unfortunately, due to the nature of the passive RFID architecture, cloned tags lower the overall accuracy of the system and may allow unauthorised personnel access to sensitive areas/information. To combat this considerable threat, we have proposed a cleaning algorithm designed specifically to identify and flag potential intrusions utilising intelligent analysis coupled with Non-Monotonic Reasoning. We conclude this research by analysing the potential benefits and drawbacks within our proposed methodology.**

I. Introduction

Radio Frequency Identification (RFID) is an automated wireless technology that utilises radio signals to track items. Tags are placed onto the object which is to be monitored and mounted readers will continually scan for said items to record the location and time of which the observation was made. Various applications utilise RFID to track important and valuable items, however, due to various issues, there is only a limited number of applications that it can be integrated into. Examples of applications that integrate RFID to improve efficiency include baggage tracking, health care and the aviation industry. One of the major concerns with RFID deployment is the security of the system when dealing with cloned tags.

Several methodologies have been put forth to detect intrusions on RFID systems. Some of these include: tag deactivation, encryption and mutual authentication. However, none of these methodologies have attempted to clean ambiguous false-positive anomalies while detecting intrusions. Likewise, none of the duplicate RFID observation cleaning software such as manual cleaning, rule defining and smoothing filter take into consideration an ambiguous intrusion detection scenario.

To counter this ambiguous problem, we proposed an enhancement to a cleaning tool that incorporates intelligence to correctly determine if a set of suspicious readings are duplicate observations or an intrusion. We have done this by using Non-Monotonic Reasoning to investigate information regarding the suspicious entry. This leads to the suspicious observations identified as either to be deleted or alerted as an intrusion. We conclude that our proposed methodology has the following distinct advantages over current state-of-the-art approaches:

- Being deterministic, it will not introduce artificial anomalies.
- Applying at a deferred stage allows our concept to have access to information not found in real-time systems.
- Our approach cleans duplicate entries and also intelligently checks if the suspicious reading is an intrusion by consulting the Non-Monotonic Reasoning engine before an action is taken.
- Due to the way the system is built, our approach will decrease the amount of data temporally.

The remainder of this paper is structured as the following: Section II will provide relevant information regarding RFID, Intrusion Detection and Non-Monotonic Reasoning while Section III will examine current solutions found in literature to detect intrusions in RFID systems. We then propose our methodology within Section IV followed by an analysis of our approach in Section V. We conclude this paper in Section VI and propose future work to continue this research area.

II. Background

Radio Frequency Identification (RFID) technology relies on radio transmissions between mountable tags and readers to automatically track items in various locations. Unfortunately, due to the issues surrounding both the data recorded and security problems with regards to intrusions, RFID systems have been integrated into only a small amount of the various applications it could be used in. Highly effective classifiers such as Non-Monotonic Reasoning may be utilised as a means to counter such ambiguities.

A. RFID

Radio Frequency Identification (RFID) refers to the seamless tracking of items by means of radio transmissions. Essentially, a tag is placed on what is to be tracked and, as it passes within the vicinity of a reader, a timestamp along with the tag and reader identifiers are passed through middleware and recorded in the data warehouse as seen in Figure 1. This results in a database filled with multiple entries of

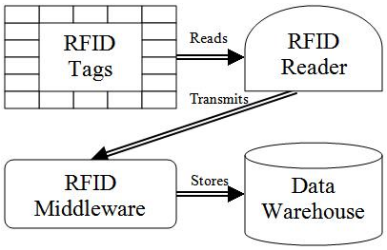

Fig. 1. A high-level representation of the data transfer among the various components of the RFID system.

observations containing the tag's identifier known as EPC (Electronic Product Code), the time at which it took place and the identifier of the reader that scanned the tag. Currently, RFID has been implemented in a vast number of activities such as supply chains [1] and health care [2]. Unfortunately, due to certain issues, RFID has only been integrated into a fraction of the applications in which it could be utilised.

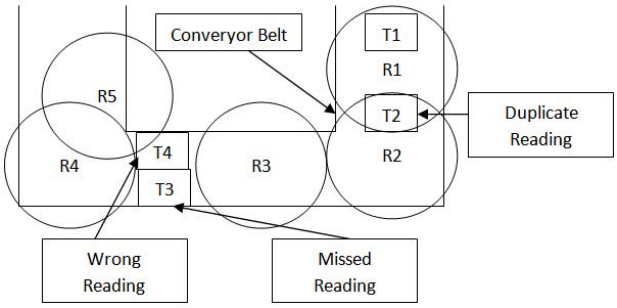

Fig. 2. A conveyor belt RFID example illustrating how a Duplicate, Missed and Wrong readings may occur.

There are four main contributing issues that prevent the commercial wide-scale adoption of RFID. These include the data being too low-level to be meaningful [3]; the error-prone nature of the incoming observations [4]; mass volumes of information being generated [5]; and complex spatio-temporal readings due to increasingly advanced technology utilised [6]. Of these issues, the data anomalies generated within the data sets is one of the most difficult issues to rectify. These errors include missing observations, wrong readings and duplicate recordings [7], [8]. Figure 2 demonstrates how various anomalies can be produced. In this example, T2 is actually producing a duplicate reading as it is meant to only be read by either R1 or R2, not both. T3 is producing a missed read as it is not read at all and T4 is a wrong read being that it is read by R5 where it is supposed to be recorded at R4. The observations that would be recorded and the correct readings may be viewed in Table I.

There are three main types of tags that are utilised within RFID systems, they include passive, semi-active and active. The passive tag relies on scavenging electromagnetic energy sent out by the RFID reader to give it enough strength to send out its own unique identifier. Due to its scavenging power source, it causes the most anomalies but also theoretically has

TABLE I
THE RECORDINGS THAT TOOK PLACE FROM THE EXAMPLE IN FIGURE 2 AND THE OBSERVATIONS THAT SHOULD HAVE BEEN RECORDED.

What is Recorded		
Tag EPC	**Timestamp**	**Reader ID**
T1	24/08/2010 12:05:01	R1
T2	24/08/2010 12:05:01	R2
T2	24/08/2010 12:05:01	R2
T4	24/08/2010 12:05:01	R5
What is supposed to be Recorded		
Tag EPC	**Timestamp**	**Reader ID**
T1	24/08/2010 12:05:01	R1
T2	24/08/2010 12:05:01	R2
T3	24/08/2010 12:05:01	R3
T4	24/08/2010 12:05:01	R4

the longest life-span.

The semi-active tag utilises a battery only to enhance the range of communication, but relies on scavenging power for sending out the signal similar to the passive tag. Due to its semi-reliance on batteries, it will eventually run out of life (5-10 years), however it will have a longer broadcasting range. The final of the three tag types is the active which relies solely on batteries to power it. It has been estimated to survive for approximately 1-5 years, but has the least amount of anomalies generated and also provides additional features that the passive and semi-active can't [9].

B. Intrusion Detection

Intrusion Detection refers to the discovering of foreign attacks upon the system usually utilising the tags that hinder the overall integrity of the data. The following five issues are some of the most dominant with regards to RFID security [10], [11]:

- **Eavesdropping:** The act of setting up an additional reader to record tag data.
- **Unauthorised Tag Cloning:** Copying tag data onto an additional tag to gain the same privileges.
- **Man-in-the-Middle (MIM) Attack:** When an external object pretends to be either a tag or reader between actual tags and readers.
- **Unauthorised Tag Disabling:** When an external reader disables a tag not allowing it to be utilised again.
- **Unauthorised Tag Manipulation:** Manipulating the tag data using an external reader.

Within this paper, we focus on the use of Tag Cloning in our scenario to gain access to privileged areas and/or information not meant for the public.

C. Non-Monotonic Reasoning

Non-Monotonic Reasoning (NMR) is a type of logic that allows multiple conclusions and eliminates the choices when given sufficient evidence to do so. With regards to NMR, we have chosen to investigate Clausal Defeasible Logic (CDL) as it has shown to be adequate at handling RFID applications in the past [12] [13] [14]. CDL has been designed to operate as NMR logic specifically for use within a computational

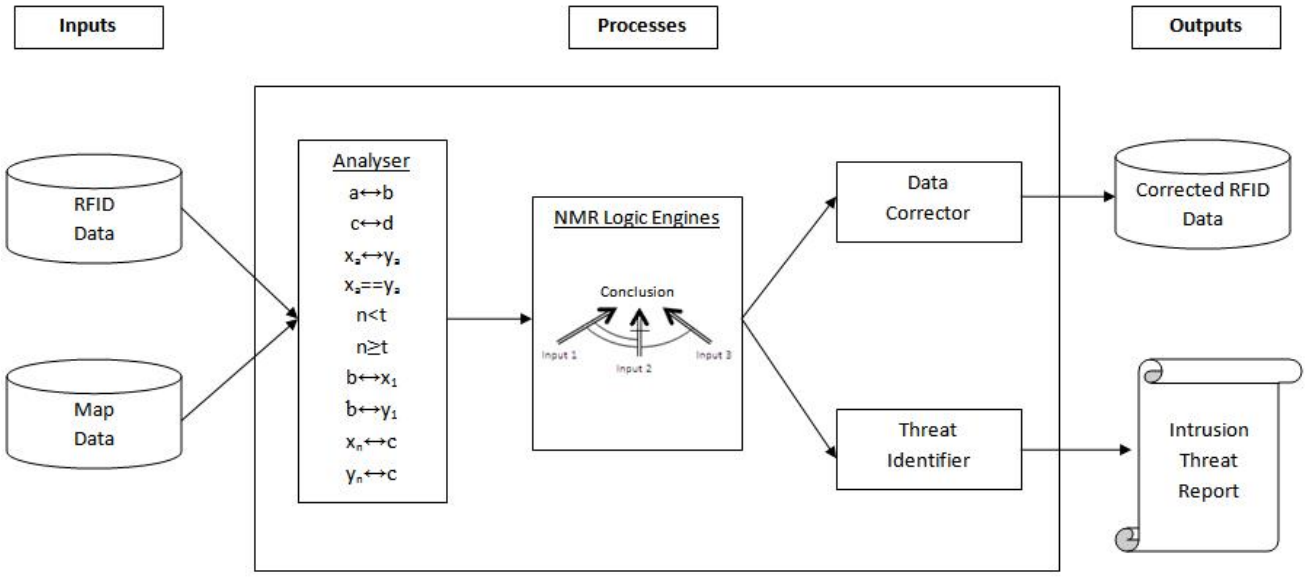

Fig. 3. The system architecture of our proposed system. Raw RFID and map data are streamed into the data analysis process. After the analysis information is gathered, the information is passed onto the Clausal Defeasible Logic engines which determine whether the suspicious readings are duplicates or intrusions.

environment and has a wide array of applications in which it may be utilised in [15]. The embedded CDL Engines will be able to deterministically arrive at an intelligent conclusion when given various input parameters.

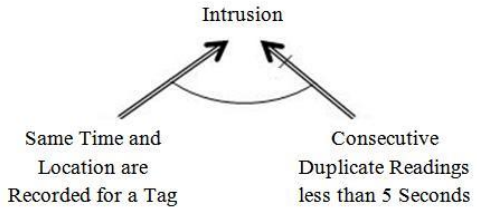

Fig. 4. A simple logic map designed to arrive at the Clausal Defeasibly correct solution when determining if a reading is an intrusion.

As seen in the RFID example in Table I, Tag T2 is recorded at two different readers at the same time. However, T2 should only be read at one location, therefore, the second recording is possibly an intrusion within the system. To represent this case within a logic map, it first needs to state the general defeasible rule that if there are two readings of the same Tag in the same place and time, it is plausible to believe it could be an intrusion. After this is done, it is necessary that a refined plausible rule which overrides the previous rule states that, if the amount of consecutive duplicate reads is less than 5 seconds, do not believe it is an intrusion. This relationship is illustrated in Figure 4 with an arch drawn to signify the rule anti-clockwise outweighs any rule clockwise of it. While there is only one conclusion that may be arrived at for each CDL Engine, it is possible to change the outcome by using stronger or weaker levels of ambiguity. CDL houses 5 various levels of ambiguity strength, which include [15]:

- μ**:** The strongest of the algorithms as it will only respond to factual information to arrive at a conclusion.
- α**:** An algorithm in which any conjunction of π and β are used to reach the conclusion.
- π**:** The algorithm in which ambiguity is propagated to reach its conclusion.
- β**:** The algorithm in which ambiguity will not be allowed to be used to draw its conclusions.
- δ**:** The formula in which the disjunction of π and β are used to draw conclusions.

To properly represent these NMR statements, the use of Decisive Programming Language (DPL) is required [16]. Within DPL, there are five symbols used to create the NMR Logic. The "$\rightarrow$" is the first which represents a Strict Rule meaning that there is no ambiguity between the input and conclusion. The second symbol is the Defeasible Rule symbol "$\Rightarrow$" which states that the conclusion is plausibly believable. The "$\rightsquigarrow$" is the Warning Rule and the third symbol we use to denote that the former entity may not disprove the latter. The final two symbols are the "$>$" which describe a priority relation, and the negate symbol illustrated as "$\sim$". Knowing the above information, the simple intrusion example mentioned above may expressed as the following:

```
R1: Same Time and Location are recorded
for a tag ⇒ Intrusion.
R2: Consecutive Duplicate Readings less
than 5 Seconds ⇒ ∼Intrusion.
R2 > R1.
```

The first general rule states that it is plausibly acceptable to believe that two readings of the same tag in the same place and time may be an intrusion. The second rule is more specific in that it states it is plausibly correct to assume that,

if there are less than 5 seconds of consecutive duplicate readings, do not conclude that it is an intrusion. The final line of the DPL coding states that the second rule stated overrides the first when both are queried. Therefore, with this knowledge, the above example mentioned in Table I without any additional knowledge would not flag the duplicate reading as an intrusion due to the reading only occurring for one second.

III. Related Work

In past literature, there have been several methodologies put forth primarily to enhance RFID security. These approaches include tag deactivation and encryption [17], mutual authentication [18], detections in tag ownership [19] and reader analysers [10]. Unfortunately, none of these methodologies consider the case in which there is an ambiguous case where a tag has been found to either be a duplicate reading or an intrusion.

Various methodologies have been proposed in the past to clean false-positive duplicate anomalies in RFID data sets. Some of these approaches include manual cleaning [20], rule defining [21] and smoothing filter [4]. None of the above mentioned cleaners consider the case in which an ambiguous false positive anomaly is actually an intrusion into the network using false tag data. Most rule-based automated cleaners will acknowledge the false-positive anomaly and proceed to delete it. However, in the event in which an intrusion has occurred, the automated processes will erase data of the breach. We would like to address this issue by specifically designing our false-positive cleaner to account for intrusions and alert the user when it occurs.

Due to the lack of integration between Intrusion Detection Systems and Duplicate RFID anomaly cleaners, we have proposed a unique system that will detect highly ambiguous intrusions through intelligent analysis and reasoning.

IV. Proposed Methodology

Our proposed methodology's architecture may be viewed in Figure 3. As depicted, the system is broken into three parts: the inputs; processes; and outputs. The inputs include Raw RFID and Map Data whereas the processes include the Analyser, Non-Monotonic Reasoning Logic Engines, Data Corrector and Threat Identifier. The two outputs we have designed include the Corrected RFID Data and the Intrusion Threat Report.

A. Motivation

Originally, we set out with the goal to devise a system that would detect intrusions using cleaning algorithms. We found that past literature has produced adequate cleaners that would detect and remove false-positive RFID data anomalies, however lacked any additional features to detect an intrusion and isolate it to present to the user. Additionally, past approaches have also been utilised to detect intrusions, however lacking the ability to decipher if an event was an intrusion or in fact a set of false positive anomalies in the system setting off costly false alarms.

Given these current trends and limitations, we were motivated to create a system to combine the integrity of cleaning with the security of an Intrusion Detection System to generate a novel approach. This resulted in us developing a system that is harnessed at a deferred stage of the cleaning cycle that intelligently analyse suspicious observations and either correct the anomalies or flag a potential intrusion threat. We attempted to utilise Non-Monotonic Reasoning engines to enhance the efficiency in our methodology when distinguishing between false-positive anomalies and intrusions.

Specifically, with regards to precious work, the manual cleaner lacks the automation to clean large sums of observations; the rule-based approach lacks the higher level of intelligence needed to handle ambiguous false-positive anomalies; and the filtration approach only cleans immediate records therefore lacking the analytical information to properly determine if the anomaly is an intrusion. We hope to improve on these weaknesses by providing an automated intelligent system that utilises readings both prior and after the suspicious observation to accurately correct the data. We also utilise effective analysis by finding values around the suspicious reading and determining certain characteristics of these values (i.e. "Are the two previous reader values equal?").

B. Analysis Process

The first process that the system is designed to examine the data sets, flag suspicious items and analyse the data surrounding the readings. It first examines each individual tag's movements throughout an environment ordered chronologically. A visual representation of this "Tag Stream" along with the various values we analyse may be viewed in Figure 5. The system will flag a reading as suspicious if there are a number of user-specified consecutive readings with the same timestamp or within a user-specified interval threshold. As default, we believe that an adequate number of consecutive misreadings is 3 and the threshold should be set at least in 5 second intervals as we believe that any consecutive reads lasting over 3 or 5 seconds is suspicious. The map data, which includes a list of readers that are within geographical proximity to each other, is needed for this part of the system.

TABLE II
Each of the checks and explanation describing each one.

Check	Explanation
a↔b	Readers 'a' and 'b' are geographically close.
b↔x_1	Readers 'b' and 'x_1' are geographically close.
b↔y_1	Readers 'b' and 'y_1' are geographically close.
x_a↔y_a	Average of Readers in 'x' and 'y' values are close.
x_a==y_a	Average of Readers in 'x' and 'y' values are equal.
x_n↔c	Readers 'b' and 'x_1' are geographically close.
y_n↔c	Readers 'b' and 'x_1' are geographically close.
c↔d	Readers 'c' and 'd' are geographically close.
n<t	The amount of readings 'n' is less than time 't'.
n≥t	The amount of readings 'n' is equal to time 't'.

The system will then group the duplicate readings by proximity and time, thereby producing a division in the tag stream as seen in Figure 5. The values examined include the

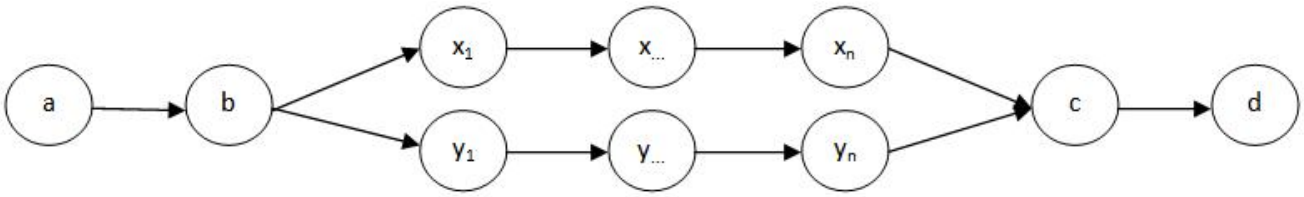

Fig. 5. A visual representation of a tag divided from others and the various components that are analysed once a suspicious set of values is discovered. '*a*', '*b*', '*c*' and '*d*' all refer to reader values while 'x_i', 'y_i' refers to the two sets of identical data streams that can either be duplicate anomalies or intrusions.

two values before the suspicious readings (*a* and *b*), the two readings after (*c* and *d*), and the values in both the suspicious tag streams (x_1-x_n and y_1-y_n). After these values have been found, the following checks are made.

Please note that the x_a refers to the average of x, x_n is the last value of the x stream which is similar to y, t refers to a user-specified threshold of acceptable consecutive duplicate readings and ↔ refers to being within geographical proximity in accordance to the map data. The == is used to determine if the values on the left and right are equal. After this analysis has been performed, all values are then passed into the Non-Monotonic Reasoning Engine.

C. Non-Monotonic Reasoning Engine

TABLE III
THE LOGIC TABLE FOR CONCLUSION 1: X = REAL ⋀ Y = INTRUSION.

Proof	Variables	Strict Rule
∼XRYI	x_a==y_a⋀n<t	Yes
XRYI	a↔b⋀c↔d⋀b↔x_1⋀x_n↔c⋀n≥t	Yes
∼XRYI	x_a==y_a	No
XRYI	b↔x_1⋀x_n↔c	No
∼XRYI	x_a↔y_a	No

For our proposed methodology, we have designed the integration of Clausal Defeasible Logic to be utilised as the Non-Monotonic Reasoning for intelligence. With regards to the determination that our Non-Monotonic Reasoning Engine can produce, we have found that there are only three possible conclusions. These include:

- x = Real ⋀ y = Intrusion (XRYI)
- x = Intrusion ⋀ y = Real (XIYR)
- x = Real ⋀ y = Real (Duplicated streams) (XRYR)

Note that there is no instance in which both x and y streams are intrusions. This is due to the fact that we assume that at least one of the suspicious streams is a real set of observations. The various analysis values used for proving or disproving a conclusion is listed in tables III - V. All of the rules are in order of precedence, 1 being the highest, and are defeasible rules unless explicitly stated as a strict rule. As default, the engine will award the "x = Real ⋀ y = Real" as true if no other conclusions are reached. If multiple conclusions are reached, the order of precedence that the system will award the determination to is "x = Real ⋀ y = Real" being highest followed by "x = Real ⋀ y = Intrusion" and "x = Intrusion ⋀ y = Real".

TABLE IV
THE LOGIC TABLE FOR CONCLUSION 2: X = INTRUSION ⋀ Y = REAL.

Proof	Variables	Strict Rule
∼XIYR	x_a==y_a⋀n<t	Yes
XIYR	a↔b⋀c↔d⋀b↔y_1⋀y_n↔c⋀n≥t	Yes
∼XIYR	x_a==y_a	No
XIYR	b↔y_1⋀y_n↔c	No
∼XIYR	x_a↔y_a	No

TABLE V
THE LOGIC TABLE FOR CONCLUSION 3: X = REAL ⋀ Y = REAL (DUPLICATE STREAMS).

Proof	Variables	Strict Rule
XRYR	x_a==y_a⋀n<t	Yes
∼XRYR	n≥t	No
XRYR	x_a↔y_a	No
∼XRYR	Default	No

D. Data Corrector/Threat Identifier

The final processes that will be run by the system will be to either report the suspicious readings as an intrusion or to delete them as duplicate readings. With regard to the deletion process, our concept has been designed to either overwrite the original data warehouse entries if the user has complete confidence in our system or to create a new and separate data warehouse. The intrusion threat report will store the timestamps, which tag has been used and where the intrusion has taken place with regard to readers.

E. Scenario and Assumptions

The system described within this research has been built to correctly clean duplicate data and detect intrusions within an enclosed building that houses privileged areas limited to certain personnel. Examples of the buildings which would house such a system include universities, hospitals and corporations. We are attempting to correct scenarios in which a building's systems are being circumvented due to an intruder claiming to have access to areas/information that they are not meant to. Real world examples of this scenario would include a corporation having trade secrets stolen by unauthorised personnel or hospitals in which people may be able access to restricted drugs not intended to be available to them.

With regard to the proposed system, we have designed it to be utilised where specific conditions are assumed. The first condition is that the environment, in which the system is utilised, is static. This is to ensure that the map data

provided to the system will be current, thereby making all further functions that require it have the highest integrity. The second condition is that the readers read at specific intervals (i.e. 5, 10 or 30 seconds). This interval value is used within the analysis and Non-Monotonic Reasoning parts of our system to determine if the suspicious reading is a duplicate.

V. Analysis

We have identified four core advantages from our observations of the methodology. The first is that our methodology is deterministic in nature which will, in turn, be unlikely to artificially introduce anomalies as other probabilistic approaches would. The second is that, by applying our concept at a deferred stage, it allows us to analyse crucial information not normally gained in real-time systems. The third advantage we have identified is that our concept will either clean a duplicate while scanning for intrusions, making it both an effective cleaner and threat detector. The final benefit we have found is that, with the interval threshold in place, our methodology will reduce the amount of temporal readings, thereby reducing the already large volume of data.

We have also identified three potential drawbacks of utilising our system. The first disadvantage is that our system is deferred and not able to flag threats in real-time. The second issue is that, being deterministic, our system cannot learn new applications as easily as a Bayesian or Neural Network would. The final potential flaw we have identified is that our system can only be utilised within a static known environment.

VI. Conclusion

Throughout this research, we have put forth a concept that utilises an intelligent RFID anomaly cleaner to also detect ambiguous intrusions. We believe that there was a need for such a technique to effectively clean false-positive data while detecting intrusions resulting in a greater level of integrity and less false alarms raised by the system. Specifically, we have identified the following as the main contributions we have made to this field of study:

- We investigated the problem of Intrusion Detection among RFID systems and identified the need for an intelligent methodology.
- We have integrated Non-Monotonic Reasoning and efficient analysis to clean duplicates while also detecting intrusions.
- We have examined the benefits and potential drawbacks of our concept.

With regard to future work, we have identified the following as potential extensions to our research. First, we would like to assess the strength of each Non-Monotonic Reasoning formulae and compare it to state-of-the-art probabilistic methods such as Bayesian and Neural Networks. We would also like to modify our concept to function in real-time and, if possible, in a dynamic environment in which some, if not all, readers are not mounted onto walls. Finally, we would like to incorporate the ability process more than two duplicate readings and integrate this research into other RFID cleaners (such as missing and wrong data).

Acknowledgment

This research is partly sponsored by ARC (Australian Research Council) grant no DP0557303.

References

[1] R. Derakhshan, M. E. Orlowska, and X. Li, "RFID Data Management: Challenges and Opportunities," in *RFID 2007*, 2007, pp. 175 – 182.

[2] C. Swedberg, "Hospital Uses RFID for Surgical Patients," RFID Journal, July 2005, available from: <http://www.rfidjournal.com/article/articleview/1714/1/1/> [Accessed: 5th June 2008].

[3] N. Khoussainova, M. Balazinska, and D. Suciu, "Probabilistic RFID Data Management," *UW CSE Technical Report UW-CSE-07-03-01*, March 2007.

[4] S. R. Jeffery, M. N. Garofalakis, and M. J. Franklin, "Adaptive Cleaning for RFID Data Streams," in *VLDB*, 2006, pp. 163–174.

[5] M. Raskino, J. Fenn, and A. Lenden, "Extracting Value From the Massively Connected World of 2015," Gartner Research, Tech. Rep. G00125949, April 2005.

[6] F. Wang and P. Liu, "Temporal Management of RFID Data," in *VLDB*, 2005, pp. 1128–1139.

[7] Y. Bai, F. Wang, and P. Liu, "Efficiently Filtering RFID Data Streams," in *CleanDB*, 2006.

[8] B. Carbunar, M. K. Ramanathan, M. Koyuturk, C. Hoffmann, and A. Grama, "Redundant Reader Elimination in RFID Systems," in *SECON*, 2005.

[9] S. S. Chawathe, V. Krishnamurthy, S. Ramachandran, and S. E. Sarma, "Managing RFID Data," in *VLDB*, 2004, pp. 1189–1195.

[10] G. Thamilarasu and R. Sridhar, "Intrusion Detection in RFID Systems," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, nov. 2008, pp. 1 –7.

[11] A. Mitrokotsa, S. Rieback, and A. Tanenbaum, "Classifying RFID Attacks and Defenses," *Special Issue on Advances in RFID Technology, Information Systems Frontiers*, July 2009.

[12] P. Darcy, B. Stantic, and R. Derakhshan, "Correcting Stored RFID Data with Non-Monotonic Reasoning," *Principles and Applications in Information Systems and Technology (PAIST)*, vol. 1, no. 1, pp. 65–77, 2007.

[13] P. Darcy, B. Stantic, and A. Sattar, "A Fusion of Data Analysis and Non-Monotonic Reasoning to Restore Missed RFID Readings," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on*, 2009, pp. 313–318.

[14] P. Darcy, B. Stantic, and A. Sattar, "Correcting Missing Data Anomalies with Clausal Defeasible Logic," in *Advances in Databases and Information Systems (ADBIS)*, 2010, pp. 149–163.

[15] D. Billington, "Propositional Clausal Defeasible Logic," in *European Conference on Logics in Artificial Intelligence (JELIA)*, 2008, pp. 34–47.

[16] D. Billington, V. Estivill-Castro, R. Hexel, and A. Rock, "Non-monotonic Reasoning for Localisation in RoboCup," in *Proceedings of the 2005 Australasian Conference on Robotics and Automation*, C. Sammut, Ed., December 2005.

[17] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems," NIST Special Publication, April 2007.

[18] D. M. Konidala, Z. Kim, and K. Kim, "A simple and cost-effective RFID tag-reader mutual authentication scheme," in *International Conference on RFID Security (RFIDSec)'07*, 2007, pp. 141–152.

[19] L. Mirowski and J. Hartnett, "Deckard: A System to Detect Change of RFID Tag Ownership," *International Journal of Computer Science and Network Security*, vol. 7, no. 7, pp. 89–98, July 2007.

[20] V. Raman and J. M. Hellerstein, "Potter's wheel: An interactive data cleaning system," in *VLDB*, 2001, pp. 381–390.

[21] J. Rao, S. Doraiswamy, H. Thakkar, and L. S. Colby, "A Deferred Cleansing Method for RFID Data Analytics," in *VLDB*, 2006, pp. 175–186.