International Journal of Applied Research in Mechanical Engineering

Volume 1 | Issue 1 Article 6

July 2011

# Semantic Ids Using Wireless Sensor Network

K. Sri Ganesh
*Department of Information Technology, Madras Institute of Technology, Anna University*,
gane884119@gmail.com

# Semantic Ids Using Wireless Sensor Network

**K. Sri Ganesh[#1], M. Raja Sekar[#2], V. Vaidehi[#3]**
*[#1,3]Department of Information Technology, [#2]Department of Electronics Engineering*
*Madras Institute of Technology, Anna University*
*Chennai, India*
*gane884119@gmail.com*

***ABSTRACT - Emerging technologies have metamorphosed the nature of surveillance and monitoring application, but the sensory data collected using various gadgets still remain changeable and poorly synchronized. An event detected by WSN formulates patterns. The sink receives the information about several events happening in the coverage area. Sink has to correlate these streaming data (events) in spatial domain (several sensors) and time domain. This paper proposes a scheme to formulate patterns based on sensing elements and a methodology for detecting an intruder using rule-based semantics. This scheme can be integrated with the surveillance systems to detect the entry of an unauthorized person into a secured area. Real Time implementations prove that events, patterns, rules can efficiently detect an intruder with the help of a wired network with appropriate database. The semantic rules are developed using ANTLR tool.***

***Key words: Wireless Sensor Network (WSN), Intrusion Detection System (IDS), ANTLR.***

## I.INTRODUCTION

Recent advancements in wireless communication and electronics have enabled the development of low cost wireless sensor networks [1]. Sensor networks are one such technology which provide enhanced intrusion detection capabilities at lower cost and reduced power consumption. One of the key advantages of WSN is their ability to bridge the gap between the physical and logical world, by gathering certain useful information from the environment and communicating the collected information to powerful devices for further data processing. It can be used to monitor the environment, detect, classify, and locate specific events and track targets over a specific region [2]. Pramod et al [2] developed a system with enhanced intrusion detection capabilities that includes event based video surveillance & recording, remote mapping of location for tracking and identification of human & metallic objects, support for real time surveillance and improved alarm functionalities. This system is capable of providing high detection capabilities with minimum false alarm rates and is adaptable to different environments. The existing scheme [2] lacks the support of knowledge base system and it fails to predict the upcoming events.

In this paper a semantic intrusion detection system (SIDS) is proposed where the information about a person's path in the surveillance system from various sensors are meaningfully correlated in time and spatial domains to detect intrusions. The outputs from the different sensors are represented as states and patterns which are then semantically analyzed by using pattern matching techniques in data mining for intrusion identification. The semantic pattern matching rules are developed using ANTLR tool [3]. The proposed SIDS has been validated using state transition analysis method. To reduce the information inaccuracy, various data mining machine leaning techniques have been used in Audit Data Analysis and Mining [4] [5].

The state transition analysis method presented in this paper is a rule based identification approach. This technique can be used to represent, identify the requirements and to compromise the penetration for only those critical events that must occur [6]. By using the information contained in a system's audit trial as input, and analysis tool can be developed to compare the state changes of the person. False positives and false negatives are the supplementary issues in surveillance security. Anomaly detection identifies activities that vary from authenticated users. It involves the creation of knowledge bases that contain the profiles of the monitored activities. JES (Java Expert System) tool is used for knowledge base. Jess is a rule engine for the Java platform [7].

This paper is organized as follows: Section II describes the related work on intrusion detection using data mining techniques. Section III presents the proposed work. Section IV presents the results and section V concludes the paper.

## II. RELATED WORK

This section discusses some of the existing works that emphasize the use of data mining techniques for intrusion detection. Ye Changguo et al [8] describes the wireless network intrusion detection algorithm based on association rule mining and expresses the feasibility of the application of fuzzy association rules mining algorithm for wireless network intrusion detecting. Hui Yang et al [9] describes data mining as the process of discovering hidden and meaningful knowledge in a data set and also highlights the

application of data mining techniques in various real-life circumstances like web personalization, network intrusion detection, and customized marketing. Idris et al [10] discusses the scope for the use of data mining technologies in intrusion detection systems for more efficient and accurate detection of various attacks in wired as well as wirelesses networks.

## III. PROPOSED WORK

Rule-Based analysis in SIDS relies on sets of predefined rules that are provided by an administrator. The rules are defined for the various application layer threats that are found in the network [4]. The rule base consists of rules that are formulated to characterize the behavior of a normal person. The rules stored in the rule base are usually in the form of if (condition) then (action). The attacks are identified by the IDS by comparing the sensed information with the various rules defined in the rule-base. In pattern matching the events that do not match with the pre-defined patterns are recognized as anomalous. In state transition analysis, penetration is viewed as sequence of actions performed by an intruder that begins from some initial state to a target comprised state on a surveillance system. A state is a snapshot of the system representing all of its authorized, unauthorized and intermediate states of the person.

### A) PATTERN MATCHING

Pattern Matching is a technique in automated data analysis, by which a group of characteristic properties of an unknown object is compared with the comparable groups of characteristics of a set of known objects, to discover the identity or to make a proper classification of the unknown object. A rule is simple a sequence of instructions which describes a particular pattern, an event should match.
ANTLR stands for Another Tool for Language Recognition. It combines lexical analysis and parsing, and uses the top-down parsing technique. ANTLR specifies its lexical rules and parser rules using almost the same notation.

ANTLR uses the notions,

a) (*Expression*)* - indicates that the expression in the parentheses must match zero or more times.
b) (*Expression*)+ - indicates that the expression in the parentheses must match one or more times.
c) (*Expression*)? - indicates that the expression in the parentheses must match zero or one times.

ANTLR takes a grammar that specifies a language as input and generates source code for a recognizer for that language, as output. It provides a single reliable notation for specifying lexers and parsers. Generally, ANTLR reads a grammar and generates a recognizer for the language defined by the grammar as shown in Figure 1.

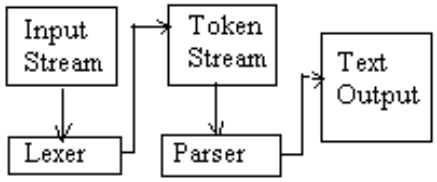


***Figure 1: ANTLR***

If there are no syntax errors then the default action would be to exit without printing any message. Actions can also be attached to the grammar elements in the grammar. These actions are written in the Java programming language in which the recognizer is being generated. When the recognizer is being generated, the actions are set in the source code of the recognizer at the suitable points.

### B) LEXICAL ANALYSIS WITH ANTLR

A *lexer* breaks up an input stream of characters into vocabulary symbols for parser. The parser relates the grammatical structure to the symbol stream. ANTLR also employs a similar recognition mechanism for lexing, parsing, and tree parsing. ANTLR generated lexers are much stronger than DFA based lexers.

The overall structure of a lexer,

```
class MyLexer extends Lexer
constructor
        {
        Variable declarations
        }
    lexer class members
    lexical rules
```

### C) LEXICAL RULES

Rules defined within a lexer grammar must have a name beginning with an uppercase letter. These rules discreetly match characters on the input stream as an alternative of tokens on the token stream. Referenced grammar elements consist of token references, characters, and strings. Lexer rules are processed in the same way as the parser rules and hence may specify arguments and return values; further, lexer rules can also have local variables and use recursion.

Grammar Rule selection

@parser:: header { }
@lexer:: header { }
[RULES SECTION]
<pattern> { <action to take when matched> }
<pattern> { <action to take when matched> }

Patterns are specified by regular expressions. Figure 2 presents the ANTLR programing structure in the form of sections.

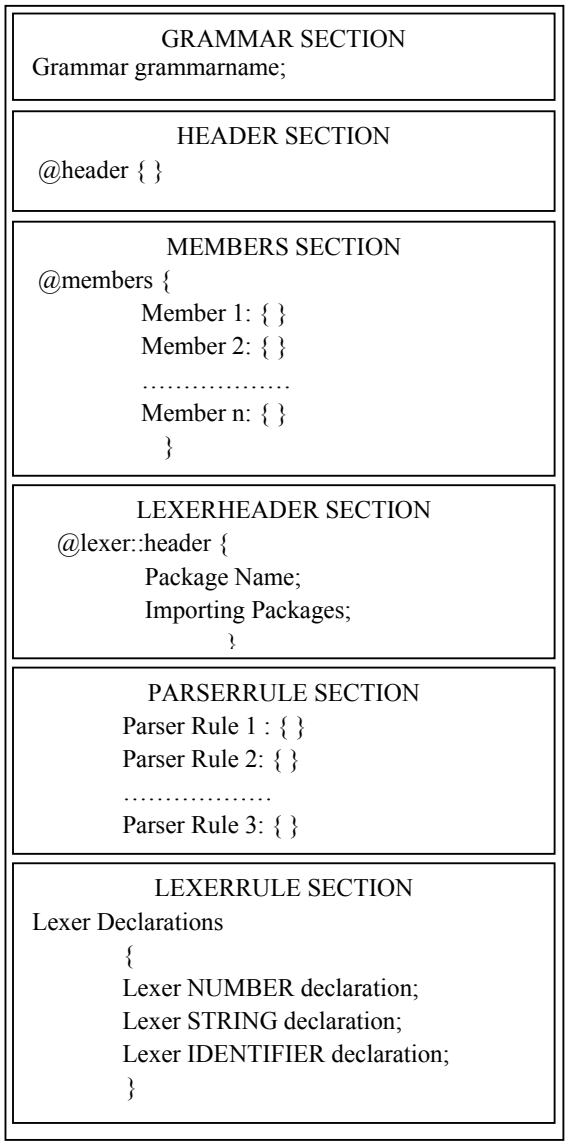


Figure 2: ANRTLR Grammar Programming Structure

In this project, PIR sensors, RFID sensors, GPS (Global Positioning System) receivers and timers are used for information gathering. RFID sensor reads the RFID tag information. PIR sensor detects the person's movement. GPS receiver provides the location of the deployed node. For our analysis number of sensors is limited to 100. Figure 3 presents the set theory notation of action and rules for SIDS algorithm.

**ALGORITHM**

INITIALIZATION

F: Field
S: Sensor

DECLARATIONS

S1, F1 : Sensor id <1 to 100>
S2, F2 : RFID range <4digits>
S3, F3 : PIR – Boolean (0, 1)
S4, F4 : GPS (X range, 4 digits; Y range, 4 digits; Z range, 4 digits)
S5, F5 : Time Stamp <8 digits>
S6, F6 : Image
F7 : Path <10paths, in each path 6 sensors>

ACTIONS

A1: Authorized to move.
A2: RFID reader failed.
A3: GPS failed.
A4: Camera malfunction
A5: Sensor node may be failed.
A6: Image recognition.
A7: Violating rules
A8: Alert the administrator.
A9: Intruder.

PROCEDURE

P1: Valid F2, perform A6 between F6 and F2's image in DB if matches A1 else perform A6 between F6 with whole DB images, if matches A7, A8 else A9.
P2: Valid F2 & !F6 (no image), get F6 from neighboring sensor nodes in the range S3±Δd during S4-Δt interval. If any F6 matches with F2's image in DB by performing A6 then A1, A4 else A8.
P3: Invalid F2, perform A6 between F6 and DB images, if matches A1, A7, A8 else A9.
P4: Invalid F2 & !F6, get F2 & F6 in the range S3±Δd during S4-Δt interval and check F2 with preceding F2, if matches perform A6 between F6 and DB images, if it matches A4, A7, A8 else A9 else A8, A9.
P5: F2, perform A6 between F6 and DB images, if matches A1, A2, A8 else A9.
P6: F2 &! F6 then A5 or A9, A8.

***Figure 3: Algorithmic representation of SIDS***

## IV. RESULTS AND DISCUSSION

In this paper, the streaming data from the sensor nodes are sent to the pattern matching tool to generate alerts based on the rules. Figure 4 and Figure 5 present the Parser rule and Lexer rule to identify whether or not the person is an intruder.

```
is    returns [String expr1]:    'IS SENSOR'
            (
      c=NUMBER 'GREATERTHAN' d=NUMBER
                              {setAnss($c.text,$d.text); }
            |
                    c=NUMBER 'SMALLERTHAN'
             d=NUMBER {setAnss($d.text,$c.text); }
            )
            {$expr1=answer1 ;};

iss    returns [String expr]:    'IS RFID'
            (
                    a=NUMBER 'GREATERTHAN'
                                        b=NUMBER
                                {setAns($a.text,$b.text); }
            |
                    a=NUMBER 'SMALLERTHAN'
              b=NUMBER {setAns($b.text,$a.text); }
            )
            {$expr=answer ;};
```

***Figure 4: Parser Rules for SIDS***

```
NUMBER    : (DIGIT)+ ;
STRING: ('a'..'z'|'A'..'Z'|'0'..'9'|'_'|'.')+;
WHITESPACE: ('\t' | ' ' | '\r' | '\n'| '\u000C' )+     {
                    $channel = HIDDEN;              } ;

Interpolation
   :   '${' i=Identifier '}'
   ;
Identifier
   :   ('a'..'z' | 'A'..'Z' | '_') ('a'..'z' | 'A'..'Z' | '_' | '0'..
.'9')*
   ;
Escape Sequence
   :   '\\' Special Char
   ;
Special Char
   :    '"' | '\\' | '$'
   ;
Space
   :   (' ' | '\t' | '\r' | '\n')
   ;
Normal Char
   :   ~Special Char
   ;
Fragment DIGIT    : '0'..'9';
```

***Figure 5: Lexer Rules for SIDS***

For pattern analysis, only F2 and F6 fields are considered to distinguish between an intruder and a normal individual. The 8-bit bit stream is composed of the following fields: sensor node (1bit), RFID (2bit), PIR (1bit), location (1bit), time (1 bit) and Image (2bit) from left to right. Totally, there are $2^6$=64 bit streams available from which only 4 are illustrated in the Table 1. In Table 1 events are assigned to the bit streams based on the procedures given in Figure 3.

***Table 1: Pattern Analysis***

| S.NO | BIT STREAM | EVENT |
|---|---|---|
| 1 | 11111111 | RFID and Image Valid |
| 2 | 11111110 | RFID Valid, Image Invalid |
| 3 | 11111100 | RFID Valid, Image Missing |
| 4 | 10011111 | RFID Missing, Image Valid |
| 5 | 10011110 | RFID Missing, Image Invalid |
| 6 | 10011100 | RFID and Image Missing |
| 7 | 11011111 | RFID Invalid and Image Valid |
| 8 | 11011110 | RFID and Image Invalid |
| 9 | 11011100 | RFID Invalid and Image Missing |

State diagrams are used to describe the behavior of the system. Event is stated as an occurrence happening at a determinable time and place, with or without the participation of person. Figure 6 presents the state transition diagram for the SIDS system where A refers to the authorized state, B and C refer to the intermediate states and D is the intruder state. Table 2 explains the state transitions for the occurrence of events. In Figure 6 the starting state may be either A, B or C based on the bit stream.

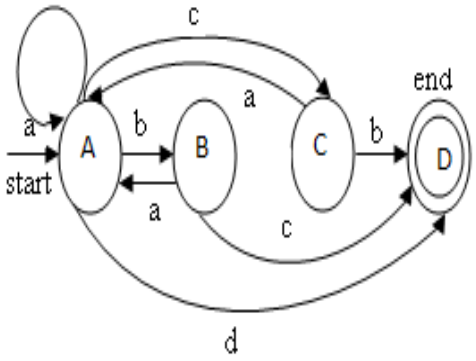


***Figure 6: State Transition Diagram***

***Table 2: Event and Event Descriptions***

| S.NO | EVENT | EVENT DESCRIPTION |
|---|---|---|
| 1 | a | RFID and Image valid |
| 2 | b | RFID Invalid / Missing |
| 3 | c | Image Invalid / Missing |
| 4 | d | RFID and Image Invalid / Missing |

Table 3 presents the Rule Pattern for the generated bit stream event and its respective decision state.

***Table 3: Rule Pattern***

| S.NO | RULE PATTERN | DECISION |
|---|---|---|
| 1 | A - A - A - A | Authorized |
| 2 | A - B - A - A | Authorized |
| 3 | B - A - A - A | Authorized |
| 4 | B - B - A - A | Authorized |
| 5 | A - C - A - A | Authorized |
| 6 | C - A - A - A | Authorized |
| 7 | C - C - A - A | Authorized |
| 8 | D - A - A - A | Authorized |
| 9 | A - B - B - B | Intruder |
| 10 | A - D - D - D | Intruder |
| 11 | A - C - C - C | Intruder |
| 12 | B - B - B - B | Intruder |
| 13 | B - C - C - C | Intruder |
| 14 | B - D - D - D | Intruder |
| 15 | C - C - C - C | Intruder |
| 16 | C - B - B - B | Intruder |
| 17 | C - D - D - D | Intruder |
| 18 | D - D - D - D | Intruder |

Using the above state analysis method, it is possible to predict a person's state efficiently.

## CONCLUSION

This paper presents a methodology for detecting an intruder using rule-based semantics**.** The state transition approach was introduced in a motive to develop an easily understandable representation of different states for detecting an intruder. Overall, the SIDS improves the security in automated surveillance systems and reduces the manpower substantially. The precision and accuracy of the system can be improved by considering all the fields in the SIDS algorithm and by the inclusion of additional states in state transition table.

## REFERENCES

***[1] Akyildiz I.F, Weilian Su, Sankarasubramaniam Y, Cayirci E,"A survey on sensor networks", Communications Magazine, IEEE , vol.40, no.8, pp. 102- 114, Aug 2002.***

***[2] Pramod P.J, Srikanth S.V, Vivek N, Patil M.U, Sarat C, "Intelligent Intrusion Detection System (In2DS) using Wireless Sensor Networks", Networking, Sensing and Control, 2009. ICNSC '09. International Conference on, vol., no., pp.587-591, 26-29 March 2009.***

*[3] Sanxian Liu, Ruisheng Zhang, Tongming Wei, Yongying He, Xianrong Su, Lian Li, "Implementing of Gaussian Syntax-Analyzer Using ANTLR", Information Science and Engineering, 2008. ISISE '08. International Symposium on , vol.2, no., pp.749-753, 20-22 Dec. 2008.*

*[4] D. Barbara, J. Couto, S. Jajodia, L. Popyack, and N. Wu, "ADAM: Detect ing intrusions by data mining", in Proc. IEEE Workshop Inf. Assurance and Security, Jun. 2001, pp. 11–16.*

*[5] K. Julish, "Data mining for intrusion detection: A critical review", IBM, Kluwer, Boston, MA, Res. Rep. RZ 3398, Feb. 2002.*

*[6] Ilgun K, Kemmerer R.A, Porras P.A, "State transition analysis: a rule-based intrusion detection approach", Software Engineering, IEEE Transactions on, vol.21, no.3, pp.181-199, Mar 1995*

*[7] Dmitry K, Dmitry V , "An algorithm for rule generation in fuzzy expert systems", Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on, vol.1, no., pp. 212- 215 Vol.1, 23-26 Aug. 2004.*

*[8] Ye Changguo, Zhang Qin, Zhou Jingwei, Wei Nianzhong, Zhu Xiaorong, Wang Tailei, "Improvement of Association Rules Mining Algorithm in Wireless Network Intrusion Detection", Computational Intelligence and Natural Computing, 2009. CINC '09. International Conference on , vol.2, no, pp.413-416,6-7June2009.*

*[9] Hui Wang, Guoping Zhang, Huiguo Chen, Xueshu Jiang, "Mining Association Rules for Intrusion Detection", Frontier of Computer Science and Technology, 2009. FCST '09. Fourth International Conference on , vol., no., pp.644-648, 17-19 Dec 2009.*

*[10] Idris N.B, Shanmugam B, "Artificial Intelligence Techniques Applied to Intrusion Detec tion", INDICON, 2005 Annual IEEE , vol., no., pp. 52- 55, 11-13 Dec. 2005.*