A Fuzzy Layered Security Management in Distributed Scheme

Seyed Mahmood Hashemi[1] Jingsha He[2]
Hashemi2138@yahoo.com jhe@bjut.edu.cn
1,2: Beijing University of Technology, School of Software Engineering
Beijing Engineering Research Center for IoT Software and Systems

*Abstract:-*This paper presents a layering system that provides security in distributed environment such as network. There is probability to vanish security relation with disability of nodes, but in proposed layering system enables to keep security relations after disability some nodes. Security relations belong to 3 different sets, so a fuzzy system combines the security rules that describe the security policy. One layer in the proposed system assign to the security rules and another layer assign to the objects in the system. Objects are grouped to security rules. Grouping the objects is done via clustering. Access requests must be sent to security layer to check and then it decides to allow them. Fuzzy clustering is used in this paper to cluster the objects for its flexibility.

Key -Words: Layering security management, fuzzy system, fuzzy clustering

1 Introduction

Security is the major issue for internet users. Security can be divided into three categories: 1-confidentially 2-integrity 3-availability. Confidentially is the concealment information or resources. Integrity refers to the trustworthiness of data. Availability refers to the ability to use the information or resource desired. Respecting to these concepts is done with number of rules, so combination of security rules is an important subject for any scheme. Since Inference Engine as major component of a Fuzzy System able to combine multi rules (2), Fuzzy System is suitable approach for combination of different rules. Another feature of Fuzzy System for security system is its flexibility.

There are many methods to solve security problem, which try to respect all aspect of security via some rules. However represented models can be sufficient for older applications, they can not response to new needs. Main reason for unreliability of older methods is their nature. Since older methods use crisp rules, they can not adopt to new situations. The best way is converting rules and situations from crisp to fuzzy. Another problem is occurred when application is used in distributed environment. Nodes in distributed environment become disabling and this is usual event. If node has security relations, they vanish with disability of node.

Fuzzy Logic allows us to define confidentially, integrity and availability in different sets, and then combine them. In other side, situation is represented with data (access requests). First of all, objects must be collected in some groups. Grouping allows us to assign suitable rules to each of them. Since there is no pre-knowledge about appropriate grouping of objects, clustering is suitable method. There are two methods for clustering objects: hard clustering and soft clustering. In hard clustering, objects are associated to clusters respected to defined thresholds. The major lack of this approach is definition of threshold. In soft clustering, suitable cluster is selected for objects. In other word, objects can belong to several clusters, but

The work in this paper has been supported by National Natural Science Foundation of China (61272500), National High-tech R&D Program (863 Program) (2015AA017204) and Beijing Natural Science Foundation (4142008).

one of them is choose. Thus if one cluster centroid become disable, other cluster centroid can replace with it. The clusters of objects include the security rules, so the requests for accessing to objects are referred to security clusters, which can decide about request according to its rules.

In this paper, a scheme for security management in distributed environment is represented. Scheme includes two sides and two layers. In the first side: the first layer is combination of security rules with Fuzzy Logic, the second layer is clusters of data. In the second side, there are list of requests. Rest of this paper is organized as follow: section 2 is about related works. Section 3 is about Fuzzy Logic and Fuzzy clustering. Section 4 describes presented algorithm and results are discussed in section 5 as conclusion.

2 Related Works

The increasing of web technologies with complexity in process is focused in [1]. Gerardo Canforda et al, represents a scenario which confidential data are more exposed unlawful disclosure, thus they proposes a three level method for confidentiality. The highest level is represented by the privacy regulation (PR). The intermediate level is the set of privacy objectives (PO), which are semi-structured statements describing how data can be accessed by users. The formulation of POs depends on the entities, the particular relationships among them, and the specific domain dictionary. The lowest layer of the model is represented by the privacy rules set which implements a given PO. A rule assumes the form of a query that the user can or can not send to database. The three layer representing is also represented in [2]. An IoT (Internet of Things) system contains tree layers: a physical perception layer that perceives physical environment and human social life, a network layer that transforms and processes perceived environment data and an application layer that offers context-aware intelligent services in a pervasive manner. Layered approach can be used in different media such as radio. In [3], layered approach is used in radio network. The cognitive radio is based on the software defined radio with adjustable operational parameters. The software allows the radio to tune to different frequencies, power levels and modulation schemes to establish or maintain a communication link. The cognitive radio network also is further adaptable to changing situation with its ability to operate successfully in collaborate or uncooperative networks. Paper analyzes attacks and mitigation techniques for both scenarios. The threats are classified according to the protocol layer upon which the attack is performed: Physical layer, Data link layer, Network layer, Application layer and cross-layer. Cross-layer attacks are those in which the attack is launched utilizing one layer while the attack targets another layer. Another aspect, which is crucial same as confidentiality, is Trust Management. [4] Proposes a scheme for dynamic trust management in P2P networks. P2P networks have the potential of converting any host into a data server and to use it as a part of a large system for disseminating information without the limitation of using a single (host) interface. A peer user usually interested to storing the downloaded file and most likely executes it. This process leaves a front door for viruses to the local host. Several interesting studies about proliferation have been presented. So they discuss the performance of the current P2P trust management strategy with consideration of internal file infection and show that file infection has the potential to underscore proliferation countermeasures. To bound virus proliferation, they propose the Double-layer Dynamic Trust (DDT) management scheme, which uses a two-layer trusting strategy aimed to alleviate the impact of the internal infection. There are number of researchers that use Artificial Intelligence tools for trust system. In [5], Trust and Reputation System (TRS) are proposed to identify trustful cooperators. Authors propose a novel and flexible Trust Computation Model (TCM) based on Artificial Neural Network (ANN) to quantify the trust relationships between agents. We propose a broker-assisting information collection strategy based on clustering method in order to improve the performance of the system. Trust of data can be examined with various approaches. For example, [6] uses a graph for trust. Onion routing networks hide user's identities behind a circuit of selected onion routers. However, they run a high risk of being compromised in the presence of the adversaries who employ malicious onion routers to perform correlation-like attacks. Exiting trust-based onion routing computes trust only according to user's own knowledge. In this paper, a novel trust graph based onion routing that mitigates key limitations in the use of trust for protecting anonymity. SGor is designed based on two key insights: 1- if people can assign trust to others according to their own knowledge independently, the trust from a group of honest people is more likely to be correct than the trust from a single honest person. 2- Although users have no immediate knowledge for their unfamiliar routers, these routers are not necessarily controlled by adversaries. Data quality approaches may be used in different types of network. In [7], data quality, which is based on cross-layered, is used in Wireless Sensor Network. In many applications of wireless sensor network (WSN) contexts the location of sensor node is important information that can be used to identify the location of an event of interest. This paper, tackles both secure localization and privacy issues in order to define an integrated solution that consider a sound privacy management policy coupled with a secure localization protocol. The presented approach is based on the assessment of data quality, which are we evaluate to which extent the information to be processed by application in reliable and trustworthy. This is done by introducing a way to evaluate the overall data quality when several cheap protection techniques are combined together. Although none of the used techniques guarantee reliability and trustworthy by itself, we exploit consistency across them to evaluate data reliability. As a result, we introduce a protocol, name cross-layer protocol (CLP) that defines fundamental steps for assessing data quality.

A common method, which is used in various aspects of security, is Clustering. A large number of clustering algorithms exist, but it is difficult to find a single clustering algorithm to get well detection effect. Fanfei Weng et al, introduce a new clustering algorithm, the Evidence Accumulation (EA) for intrusion detection based on the concept of clustering ensemble. In this approach, K-mean algorithm runs N times (as number as data) to find appropriate cluster. In [10], is used to intrusion detection. The paper proposed one kind of k-means algorithm based on the k-medics cyclic method and the improved triangle trilateral relations theorem, which improves the k-means algorithm from reduce makes the improvement to the initial cluster center dependence and the algorithm time expenses. Eduardo Raul Hruschka et al, present a survey for evolutionary algorithms in clustering [9].

Researches, which are mentioned above suffers from a number of problems and they are focus on some notes. Firstly, they can not combine the rules for different aspects of security successfully. Secondly, adaptation between access demands and rules is problem. Papers provide some notes that must be used for contribution. At the first is layering. The second subject is clustering. This technique (clustering) causes perfect partitioning. In present paper, both of them are noted.

3 Fuzzy

A *Fuzzy System* includes numbers of rules. The output of system is the result of *Inference Engine*, so inference engine allows to combination of rules. Fuzzy systems needs to definition of *fuzzy sets*.

a. Fuzzy Sets

A Fuzzy Set is characterized by a membership function which associates with each point in space of points a real number between 0 and 1 [11]. In other words, each point x in a fuzzy set A is represented by a value between zero and one and this value declare who much point x belongs to A [12].

Let a system with uncertainty have the input output relation $y = f_s(x)$, where $y \in R$, and $y \in R^{nX}$. A fuzzy system represents the knowledge related to inputs and output by nC fuzzy rules R_1, … R_C which are expressed in the form

R_i : If ($x_{k,1}$ isr $A_{i,1}$) and … and ($x_{k,nX}$ isr $A_{i,nX}$) then ($y^*_{k,i}$ isr B_i). (1)

Where $y_k=f_s(x_k)$ is an observation vector (x_k, y_k) of the system; $x_{k,j}$ is the j^{th} variable of x_k ; $A_{i,j}$ is the membership function of the fuzzy set for the j^{th} variable in the i'th rule, which determines a fuzzy number for the j'th variable of input space; $y^*_{k,i}$ is the estimate of $y_k=f_s(x_k)$ by R_i; the operator "and" denotes the *t-norm* operation between two membership values; and "isr" denotes the belonging of an object into a fuzzy set.

b. Fuzzy Clustering

Clustering is a common method in *Pattern Recognition*. When there is no pre-knowledge about data clustering is suitable approach. The objective for clustering is partition data into number clusters base on their similarities. In other words, data in specific cluster are more similar than data in two different clusters. Thus a suitable measurement is necessary for any approach of clustering. The measurement of clustering is often called *distance*. The next step in clustering is associating data to clusters base on distance. Clustering approaches divide into two categories broadly: 1- hard clustering and 2-soft clustering. In hard clustering, each data is associated to exactly one cluster. In soft clustering (or fuzzy clustering), each data may have associated to more than one cluster.

4 Proposed Scheme

There are two problems in present security schemes. Firstly, they do not suitable in distributed environment. In distributed environment, the nodes may become disabling usually. If disable node had security relations, they vanish with disability of node. Since disabilities of nodes are very usual in distributed environments (networks), the method to keep security relations is necessary. This problem can be solved with grouping and save security relations in number nodes. Fuzzy Clustering able to clusters objects and define number centers for them.

Secondly, security relations are done with a set of rules and performance of security system is related to combination of them. Fuzzy System allows us to combine many of rules perfectly.

Proposed scheme consist two sides. One side of scheme is about security of system and another side is about access demands (access requests). Security side includes two layers. The first layer presents the security policy in the system and the second layer is objects in the system. Thus the overview of system is Fig. 1.

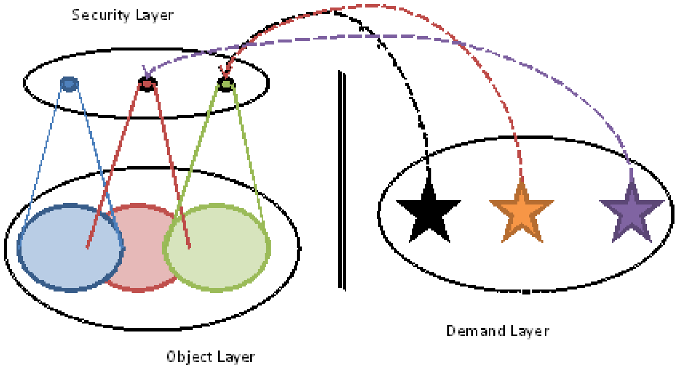


Fig. 1. Overview of Scheme

Since both of them (security policy and objects) use the fuzzy-system, the first step is converting them to fuzzy meaning. Fuzzy-system, which is used, is declared in Fig. 2.

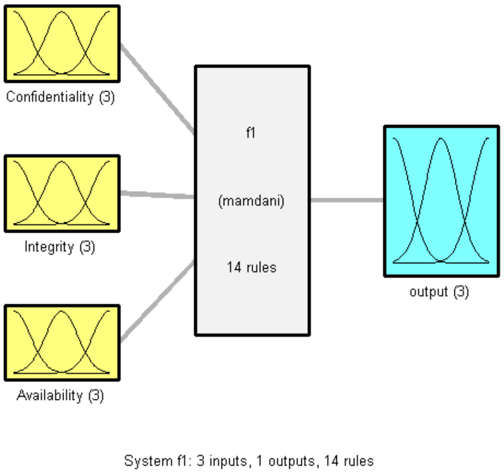


Fig. 2. Properties of fuzzy-system

Converting variables to fuzzy numbers needs to definition of Fuzzy Sets. In this system, three fuzzy sets for each concepts of security are defined. Low, Medium and High are fuzzy sets defined to keep variables and same as these sets are defined as output of fuzzy system to represent to value of inference engine as fuzzy number. Variables are represented in fuzzy systems as degree of membership functions. Fig. 3, shows the membership functions of "Confidentiality".

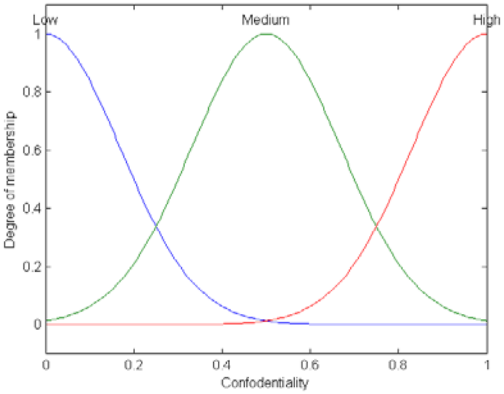
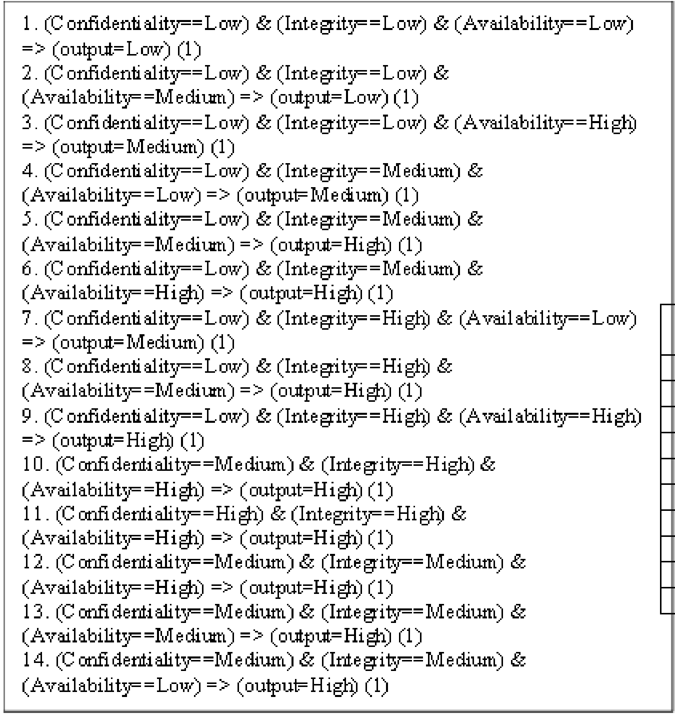


Fig. 3. Membership functions of “Confidentiality”

Membership functions of Integrity, Availability and Output of fuzzy-system are same as membership functions of “Confidentiality”. Another thing, which is necessary in fuzzy-system, is a set of rules. The set of rules represents the security policy. Each rule has three inputs (Confidentiality, Integrity and Availability) and one output.



1. (Confidentiality==Low) & (Integrity==Low) & (Availability==Low) => (output=Low) (1)
2. (Confidentiality==Low) & (Integrity==Low) & (Availability==Medium) => (output=Low) (1)
3. (Confidentiality==Low) & (Integrity==Low) & (Availability==High) => (output=Medium) (1)
4. (Confidentiality==Low) & (Integrity==Medium) & (Availability==Low) => (output=Medium) (1)
5. (Confidentiality==Low) & (Integrity==Medium) & (Availability==Medium) => (output=High) (1)
6. (Confidentiality==Low) & (Integrity==Medium) & (Availability==High) => (output=High) (1)
7. (Confidentiality==Low) & (Integrity==High) & (Availability==Low) => (output=Medium) (1)
8. (Confidentiality==Low) & (Integrity==High) & (Availability==Medium) => (output=High) (1)
9. (Confidentiality==Low) & (Integrity==High) & (Availability==High) => (output=High) (1)
10. (Confidentiality==Medium) & (Integrity==High) & (Availability==High) => (output=High) (1)
11. (Confidentiality==High) & (Integrity==High) & (Availability==High) => (output=High) (1)
12. (Confidentiality==Medium) & (Integrity==Medium) & (Availability==High) => (output=High) (1)
13. (Confidentiality==Medium) & (Integrity==Medium) & (Availability==Medium) => (output=High) (1)
14. (Confidentiality==Medium) & (Integrity==Medium) & (Availability==Low) => (output=High) (1)

Fig. 4. The rules of fuzzy-system

In the security layer, there are number of **Class-of-Security** (CoS). Each CoS is a combination of different concepts of security (Confidentiality, Integrity and Availability) which is determined by administrator of system. In other words, administrator enters different real values for ‘Confidentiality’, ‘Integrity’ and ‘Availability’. The real values proceed according to the rules. Since the fuzzy-system is “mamdani”, the resulted fuzzy values convert to real numbers. There are 3 CoS in the instant scheme. The formula for final result of fuzzy system is represented in (2) and Table 1 shows the results for numerical examples.

$$f(x) = \frac{\sum_{l=1}^{M} \bar{y}^{l} \left(\prod_{i=1}^{n} \mu_{A_i^l}(x_i) \right)}{\sum_{l=1}^{M} \left(\prod_{i=1}^{n} \mu_{A_i^l}(x_i) \right)}$$

(2)

Where M is number of rules (M=14), $\bar{y}$ is output of each rule, x_i is input, n number of inputs and μ is membership degree of each input (it has three values for ‘Low’, ‘Medium’ and ‘High’).

No. CoS	Value for ‘Confidentiality’	Value for ‘Integrity’	Value for ‘Availability’	Fuzzy Value
1	0.92	0.73	0.98	0.8182
2	0.34	0.61	0.12	0.7131
3	0.05	0.16	0.95	0.5153

Table 1. Values of CoS

In the object layer, there are number of **Class-of-Object** (CoO). Each CoO is an object of the system. Since accessing to each object needs to a degree of security, there are needed values for ‘Confidentiality’, ‘Integrity’ and ‘Availability’. Values for ‘Confidentiality’, ‘Integrity’ and ‘Availability’ are entered to fuzzy-system (with formula (2)) as real number, then fuzzy values of them is make. There are 10 CoO in the instant scheme.

No. CoO	Value for ‘Confidentiality’	Value for ‘Integrity’	Value for ‘Availability’	Fuzzy Value
1	0.90	0.18	0.903	0.7674
2	0.87	0.238	0.204	0.7799
3	0.956	0.832	0.341	0.7435
4	0.001	0.82	0.73	0.8315
5	0.8147	0.9058	0.127	0.765
6	0.9134	0.6324	0.0975	0.7618
7	0.2785	0.5469	0.9575	0.824
8	0.9649	0.9706	0.9572	0.867
9	0.4858	0.8003	0.1419	0.7563
10	0.7922	0.9595	0.6557	0.7902

Table 2. Values of CoO

CoO belongs to the clusters of CoS. Clustering approach is (soft) fuzzy, i.e. distance between CoS and CoO is evaluated, then the nearest CoS is selected as **Major-Centroid** for CoO and others **Candidate-Centroid**. Table 3 represents distance between each CoO and CoS.

No. CoO	Dist. To 1th CoS	Dist. To 2th CoS	Dist. To 3th CoS	Major-Centrid	Candidate-Centroids
1	0.0508	0.0543	0.2521	1	2,3

2	0.0383	0.0668	0.2646	1	2,3
3	0.0747	0.0304	0.2282	2	1,3
4	0.0133	0.1184	0.3162	1	2,3
5	0.0532	0.0519	0.2497	2	1,3
6	0.0564	0.0487	0.2465	2	1,3
7	0.0058	0.1109	0.3087	1	2,3
8	0.0488	0.1539	0.3517	1	2,3
9	0.0619	0.0432	0.2410	2	1,3
10	0.0280	0.0771	0.2749	1	2,3

Table 3. Major-Centroid and Candidate-Centroid for each CoO

Accessing requests from demand layer come to security level and to CoS. CoS must to process the request and allow/fail them to access the CoO.

In the distributed situation, a common event is disability of a node. If node contains security relations, they are vanished with disability of node, so security of system decrease deeply. In present scheme, problem of vanishing security relations with node disability is solved. CoS determine about accessing and each of them is kept in distinguish node. If Major-Centroid, node which keeps security relation of a CoO becomes disable, another Candidate-node replace with it. Therefore, security relations are kept in any situation (with some differences). This event is represented in Fig. 4.

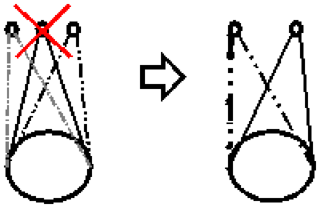


Fig. 4. Cos and CoO after node disability

5 Conclusion

Security system consists two parts. The major part of security system is rules. Rules explain the security policy. Since security policy covers various aspects of security, the numbers of rules me be exceed. Therefore a mechanism for combination of rules is necessary. System is as carefully as combination mechanism. Another aspect of optimum rules is full description of them. Fuzzy logic uses *declarative terms*, so it is suitable for security rules.

The second stage in any security management is associating objects to security rules. Clustering can be used for this task. Soft clustering can be more useful than hard clustering especially in distributed environment. Since in soft clustering any data (object) can belong to more than one cluster simultaneously and this is suitable for any non-predictive environment same as network.

References

[1]. Gerardo Canfora, Elisa Costante, Igino Pennino, Corrado Aaron Visaggio, “A Tree-Layered Model to Implement Data Privacy Policies”, ELSEVIER, Computer Standards & Interfaces, 30 (2008) 398-409

[2]. Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, “A Survey of Trust Management for Internet of Things”, ELSEVIER, Journal of Network and Computer Application, 42 (2014) 120-134

[3]. Deanna Hlavacek, J. Morris Chang, “A Layered Approach to Cognitive Radio Network Security: A Survey”, ELSEVIER, Computer Networks, 2014, http://dx.doi.org/10.1016/j.comnet.2014.10.001

[4]. Lin Cai, Roberto Rojas-Cessa, “Mitigation of Malware Proliferation in P2P Networks using Double-Layer Dynamic Trust (DDT) Management Scheme”, Supported by National Science Foundation under Grant Award 0435250

[5]. Bo Zong, Feng Xu, Jun Jiao, Jian Lv, “A Broker-Assisting Trust and Reputation System Based on Artificial Neural Network”, Proceeding of the 2009 IEEE International Conference on Systems, Man and Cybernetics, 2009

[6]. Peng Zhou, Xiapu Luo, Ang Chen, Rocky K.C. Chang, “SGor: Trust Graph based onion routing”, ELSEVIER, Computer Networks, 57 (2013) 3522-3544

[7]. Alberto Coen-Porisini, Sabrina Sicari, “Improving Data Quality Using a Cross Layer Protocol in Wireless Sensor Networks”, ELSEVIER, Computer Networks, 56 (1012) 3655-3665

[8]. Fangfei Weng, Qingshan Jiang, Liang Shi, Nannan Wu, “An Intrusion Detection System Based on the Clustering Ensemble”, IEEE, 1-4244-1035-5/07/$25.00, 2007

[9]. Eduardo Raul Hruschka, Ricardo J. G. B. Campello, Alex A. Freitas, Andre C. Ponce Leon F. De Carvalho, “A Survey of Evolutionary Algorithms for Clustering”, IEEE TRANSACTION ON SYSTEMS, MAN AND

CYBERNETICS—PART C: APPLICATION AND REVIEWS, Vol. 39, No. 2, 2009

[10]. Li Tian, Wang Jianwen, “Research on Network Intrusion Detection System Based on Improved K-means Clustering Algorithm”, IEEE, 2009 International Forum on Computer-Science Technology and Applications,

[11]. Lotfi A. Zadeh, “Fuzzy Sets”, Information and Control, 338-353, 1965

[12]. Lotfi A.Zadeh, “The birth and evolution of fuzzy logic”, International Journal of General Systems 17, 95-105, 1990

[13]. Li-Xing Wang, “A Course in Fuzzy Systems and Control”, Prentice-Hall International Inc., pp 118-127