Vehicle Network Security Situation Assessment Method Based on Attack Tree

Ruxiang Li, Fei Li and Jiayan Zhang
School of Cyberspace Security, Chengdu University of Information Technology, Chengdu 610225, China.
Email: lifei@cuit.edu.cn

Abstract. In order to solve the problem that the current vehicle network security situation assessment methods are seriously few, and the existing methods have low accuracy and are greatly affected by subjective factors, an attack tree-based vehicle network security situation assessment method is proposed. Firstly, the attack tree models are established to describe the network attacks the internet of vehicles may suffer from. Secondly, the security attributes of the attack path are determined, and each attack path is scored. At the same time, the fuzzy analytic hierarchy process is used to solve the weight values of each attack path. After that, weights and ratings are used to assess the security situation level of the threat. Finally, a comparative analysis of the security situation assessment with the analytic hierarchy process shows that the fuzzy analytic hierarchy process method can reduce the influence of human subjective factors and improve the credibility of the security situation assessment.

1. Introduction
The intelligent transportation system is one of the research hotspots in transportation field. An important part of intelligent transportation is the internet of vehicles. The internet of vehicles brings us many conveniences as well as network security threats. Some of these security threats may cause privacy leaks, and some may even lead to car crashes, so it is necessary to attach great importance to the safety of the internet of vehicles.

In the face of increasingly complex and diverse security threats to the internet of vehicles, existing security protection technologies cannot deal with them effectively. It is urgent to use Network Security Situation Awareness to monitor and protect the internet of vehicles. This technology can extract the security-related factors in the network for analysis, perceive the network security state, and predict the future situation. Network Security Situation Assessment is an important process of situational awareness and the basis of situational prediction.

Researches on network security situation assessment are gradually increasing. Yegeswaran et al. adopt honeypot technology to obtain network activity information and evaluate network security situation [1]. Sabata et al. use the multiple evidence fusion technology to complete the assessment of network security situation [2]. C.ee et al. design a visual network situation assessment system. They describe the network security situation by analyzing the intrusion detection system and firewall data [3]. Chen Xiuzhen et al. divide the network environment into system, host and service. They perceive the network security situation according to the characteristics of these parts [4]. Xu Xiaohui et al. use rule-based reasoning method and D-S theory to evaluate network security situation [5]. Hao Shuyong et al. use the rule mining method based on cloud model to depict the network security situation [6].

The existing researches on network security situation assessment methods are mainly for traditional networks. These methods are not suitable for the internet of vehicles, and have large artificial
subjective factors. Therefore, the attack tree and fuzzy analytic hierarchy process (FAHP) are employed to reduce the impact of human subjective factors and make assessment more accurately.

2. Vehicle Network Attack Tree Modeling

2.1. Concepts Related to Attack Tree Model
The attack tree model is a graphical method to describe system security. This method uses a tree structure to describe the attack path. The attack tree model contains a root node, branch nodes, and leaf nodes. The root node represents the ultimate goal of the attack, while the branch node and leaf node represent the attack methods taken to complete the attack target.

2.2. Attack Tree Modeling
We construct the vehicle network attack tree models by referring to the implementation methods of various security threats in the internet of vehicles. Since there are many systems involved in the internet of vehicles and various types of security threats for different systems, we divide the vehicle network into three parts: the inner-vehicle network part, the vehicle access equipment part, and the vehicle network communication part.

In order to describe these attack trees conveniently, the root node in attack trees are represented by $G_i (i=1,2,\ldots,n)$, the branch node are represented by $M_i (i=1,2,\ldots,n)$, and the leaf node are represented by $E_i (i=1,2,\ldots,n)$. According to these rules, the inner-vehicle network attack tree is shown in figure 1. The meaning of each node is shown in table 1. The inner-vehicle network attack tree is divided into three parts: CAN bus part, ECU part and gateway part.

![figure 1](image-url)

**Figure 1.** Inner-vehicle Network Attack Tree

| Table 1. Meaning of Each Node in the Inner-vehicle Network Attack Tree |
|-------------------|-------------------|-------------------|-------------------|
| Node             | Meaning            | Node             | Meaning            | Node             | Meaning                      |
| $G_V$            | Inner-vehicle network | $M_{v8}$        | Injection attack  | $M_{v12}$        | Man-in-the-middle attack     |
| $M_{v1}$         | CAN bus            | $M_{v7}$        | Blackhole attack  | $M_{v13}$        | Paralyze CAN bus             |
| $M_{v2}$         | ECU                | $M_{v8}$        | ECU flash         | $M_{v14}$        | Illegal control of the car   |
| $M_{v3}$         | Gateway            | $M_{v9}$        | Malicious code injection | $M_{v15}$  | Paralyze CAN bus             |
| $M_{v4}$         | Replay attack      | $M_{v10}$       | Packet tampering  | $M_{v16}$        | Tamper with ECU data         |
| $M_{v5}$         | DOS attack         | $M_{v11}$       | Packet replay attack | $M_{v17}$  | Send malicious instructions  |
Table 1. Continued

| Node   | Meaning                              | Node   | Meaning                              | Node   | Meaning                              |
|--------|--------------------------------------|--------|--------------------------------------|--------|--------------------------------------|
| Mv18   | Illegal control of the car           | Mv25   | fabricate packet content             | Ev6    | Get ECU permission                   |
| Mv19   | Send high priority packet            | Mv26   | Analysis packet content              | Ev7    | Illegal interception of packet       |
| Mv20   | Send malicious packet                | Ev1    | Send malicious packet                | Ev8    | Illegal interception of packet       |
| Mv21   | Discard normal packet                | Ev2    | Illegal interception of packet       | Ev9    | Illegal interception of packet       |
| Mv22   | Get ECU permission                   | Ev3    | Illegal interception of packet       | Ev10   | Illegal interception of packet       |
| Mv23   | Tamper with packet content           | Ev4    | Get CAN bus permission               |        |                                      |
| Mv24   | Tamper with packet content           | Ev5    | Flash tool access                    |        |                                      |

The attack tree model of the vehicle access equipment part is shown in figure 2. The meaning of each node is shown in table 2. The attack tree is divided into OBD part, TBOX part and vehicle key-free system part.

Figure 2. Vehicle Access Equipment Attack Tree

Table 2. Meaning of Each Node in the Access Equipment Attack Tree

| Node   | Meaning                              | Node   | Meaning                              | Node   | Meaning                              |
|--------|--------------------------------------|--------|--------------------------------------|--------|--------------------------------------|
| GD     | vehicle access equipment             | MD11   | Replay attack                        | MD22   | Physical illegal access              |
| MD1    | OBD                                  | MD12   | Shared function attack               | MD23   | Physical illegal access              |
| MD2    | TBOX                                 | MD13   | Bluetooth crack attack               | MD24   | DNS session hijacking                |
| MD3    | vehicle key-free system              | MD14   | Side channel attack                  | MD25   | DNS session hijacking                |
| MD4    | Tamper with data                     | MD15   | Illegal monitoring of CAN            | MD26   | Send high priority packet            |
| MD5    | Fabricate sensor messages            | MD16   | Malware implant                      | ED1    | Illegal port access                  |
| MD6    | Send malicious instructions          | MD17   | Monitor communication                | ED2    | Physical illegal access              |
| MD7    | Steal sensitive data                 | MD18   | Monitor communication                | ED3    | Illegal access to the network        |
| MD8    | Tamper with data                     | MD19   | Paralyze communication               | Ed4    | Counterfeit base station             |
| MD9    | DOS attack                           | MD20   | Intercept key signal                 | Ed5    | Counterfeit base station             |
| MD10   | Replay attack                        | MD21   | Crack key                            | Ed6    | Illegal access to the network        |
Table 2. Continued

| Node | Meaning                        | Node | Meaning                        | Node | Meaning                        |
|------|--------------------------------|------|--------------------------------|------|--------------------------------|
| $E_{D7}$ | Illegal interception of packet | $E_{D9}$ | Intercept shared key | $E_{D11}$ | Intercept key signals |
| $E_{D8}$ | Interfere with car receiving signals |         |                                |         |                                |

The attack tree model of the vehicle network communication part is shown in figure 3. The meaning of each node is shown in table 3. This part is divided into spectrum interference attack part, tunnel attack part, DOS attack part, man-in-the-middle attack part and wormhole attack part.

![Vehicle Network Communication Attack Tree](image)

Table 3. Meaning of Each Node in the Vehicle Network Communication Attack Tree

| Node | Meaning                        | Node | Meaning                        | Node | Meaning                        |
|------|--------------------------------|------|--------------------------------|------|--------------------------------|
| $G_T$ | Vehicle network communication | $M_{T7}$ | Path information miscalculated | $E_{T2}$ | Create a communication channel |
| $M_{T3}$ | Spectrum interference attack | $M_{T8}$ | Send high priority packet | $E_{T3}$ | Illegal access to the network |
| $M_{T2}$ | Tunnel attack                 | $M_{T9}$ | Steal communication data      | $E_{T4}$ | Intercept communication packet |
| $M_{T3}$ | DOS attack                    | $M_{T10}$ | Tamper with communication data | $E_{T5}$ | Intercept communication packet |
| $M_{T4}$ | Man-in-the-middle attack      | $M_{T11}$ | Interference positioning information | $E_{T6}$ | Establish a wormhole link |
| $M_{T5}$ | Wormhole attack               | $M_{T12}$ | Concealing the true path of the node |         |                                |
| $M_{T6}$ | Disrupt vehicle communication | $E_{T1}$ | Transmitting interference signal |         |                                |

3. Security Situation Assessment Based on FAHP

3.1. Concepts of Fuzzy Analytic Hierarchy Process (FAHP)
Fuzzy analytic hierarchy process (FAHP) is an improved method of analytic hierarchy process (AHP). The AHP method uses a combination of qualitative and quantitative ways to analyze the system and quantitatively describes the indicators involved in the system. The AHP method also calculates the optimal solution through mathematical methods. However, in this method, it is very difficult to check whether the judgment matrix is consistent. The commonly used consistency standard lacks scientific basis and the standard usually does not consider the judgment ambiguity of human when constructing the pairwise judgment matrix. Therefore, the fuzzy number is introduced to reduce the impact of subjective factors in the analysis process.
3.2. Scoring of Security Attributes

Security attributes can reflect the extent of an attack. Literature [7]-[9] also used the FAHP method to analyze the attack tree model. The security attributes used are: the difficulty of attack, the cost of an attack and the possibility of an attack being discovered. However, the vehicle network is more complicated and the security threats are diverse. Therefore, these three security attributes are not applicable to the analysis of the internet of vehicles attack tree. The security attributes selected in this paper are: the spread range of an attack (trans), the attack reappearance difficulty (recur), the possibility of an attack being discovered (find), and the loss of an attack can cause (lost). In order to analyze the attack tree model, the scoring criteria for the above security attributes are shown in table 4.

| Range          | Difficulty Level  | Difficulty Level | Possibility Level | Loss Level |
|----------------|-------------------|------------------|-------------------|------------|
| Extremely wide | Extremely difficult| 1                | Extremely hard   | 1          |
| Wide           | Difficult         | 2                | Hard              | 2          |
| Medium         | Medium            | 3                | Medium            | 3          |
| Small          | Easy              | 4                | Easy              | 4          |
| Extremely Small| Extremely easy    | 5                | Extremely easy    | 5          |

According to the security attribute scoring criteria of table 4, each attack path of the three attack trees is respectively scored. When scoring, the leaf nodes of each attack path represent the attack path, and the scoring results are shown in table 5, table 6, and table 7.

Table 5. Scores of Each Attack Path in Inner-vehicle Network Attack Tree

| Node | Range | Difficulty | Possibility | Loss |
|------|-------|------------|-------------|------|
| $E_{V1}$ | 3     | 2          | 3           | 4    |
| $E_{V2}$ | 2     | 3          | 3           | 4    |
| $E_{V3}$ | 3     | 3          | 3           | 5    |
| $E_{V4}$ | 3     | 2          | 3           | 4    |
| $E_{V5}$ | 2     | 3          | 3           | 4    |
| $E_{V6}$ | 4     | 3          | 3           | 4    |
| $E_{V7}$ | 2     | 3          | 3           | 4    |
| $E_{V8}$ | 3     | 4          | 3           | 4    |
| $E_{V9}$ | 3     | 3          | 4           | 5    |
| $E_{V10}$ | 3    | 3          | 4           | 5    |

Table 6. Scores of Each Attack Path in Vehicle Access Equipment Attack Tree

| Node | Range | Difficulty | Possibility | Loss |
|------|-------|------------|-------------|------|
| $E_{D1}$ | 3     | 2          | 3           | 4    |
| $E_{D2}$ | 3     | 2          | 4           | 4    |
| $E_{D3}$ | 3     | 3          | 4           | 4    |
| $E_{D4}$ | 4     | 2          | 3           | 3    |
| $E_{D5}$ | 4     | 2          | 3           | 3    |
| $E_{D6}$ | 4     | 2          | 4           | 4    |
| $E_{D7}$ | 2     | 2          | 3           | 5    |
| $E_{D8}$ | 2     | 3          | 2           | 4    |
| $E_{D9}$ | 3     | 3          | 3           | 4    |
| $E_{D10}$ | 4    | 4          | 2           | 2    |
| $E_{D11}$ | 3    | 3          | 3           | 4    |
Table 7. Scores of Each Attack Path in Vehicle Network Communication Attack Tree

| Node | Range | Difficulty | Possibility | Loss |
|------|-------|------------|-------------|------|
| $E_{T1}$ | 4     | 3          | 4           | 3    |
| $E_{T2}$ | 3     | 2          | 2           | 4    |
| $E_{T3}$ | 3     | 4          | 3           | 3    |
| $E_{T4}$ | 3     | 3          | 4           | 4    |
| $E_{T5}$ | 3     | 3          | 4           | 4    |
| $E_{T6}$ | 3     | 2          | 3           | 4    |

3.3. Security Attributes Weight Calculation

We use the FAHP method to calculate the weight of security attributes. In order to quantitatively describe the relative importance between the two security attributes, the commonly used attribute comparison scale table is shown in table 8.

Table 8. Comparison Scale

| Scale | Description                                                                 |
|-------|-----------------------------------------------------------------------------|
| 0.5   | Attribute i and attribute j have the same effect on node score              |
| 0.6   | Attribute i has a slightly greater impact on node score than attribute j    |
| 0.7   | Attribute i has a greater impact on node score than attribute j             |
| 0.8   | Attribute i has a materially greater impact on node scores than attribute j |
| 0.9   | Attribute i has an extremely greater impact on node scores than attribute j |
| 0.1~0.4 | The effect of attribute i relative to attribute j on node score is opposite to the above |

Then we compare the security attributes according to Table 8 and obtain the following fuzzy judgment matrix $C$:

$$C = \begin{bmatrix} 0.5 & 0.6 & 0.4 & 0.4 \\ 0.4 & 0.5 & 0.4 & 0.3 \\ 0.6 & 0.6 & 0.5 & 0.4 \\ 0.6 & 0.7 & 0.6 & 0.5 \end{bmatrix}$$

Since the consistency of the judgment matrix and the criteria of consistency greatly affect the final ranking result [10], it is necessary to check the consistency of the fuzzy matrix. At present, there is no unified detection method for the consistency problem of fuzzy matrices. Most of the methods are improved and adjusted around the consistency ratio $CR < 0.1$, but the reason for using this ratio is not given. Some scholars also propose transforming fuzzy judgment matrix and fuzzy consistency matrix through mathematical transformation, but such methods have the disadvantage of too much adjustment range, which cannot reflect the intention of decision makers well and cause errors. We select the method proposed in literature [10], which rigorously deduces the feasibility of using the additive consistency of fuzzy judgment matrix to determine its consistency. This paper also gives the criterion of consistency. Using this method, the fuzzy judgment matrix $C$ can be judged by equation (1).

$$d = \frac{2}{n(n-1)(n-2)} \sum_{i,j} \sum_{k \neq i,j} e_{ij} - \left( e_{ij} + e_{ij} - \frac{1}{2} \right)$$

(1)

Literature [10] believes that the smaller the additive consistency index $d$, the better the consistency of the fuzzy judgment matrix. Through calculation, the additive consistency index of matrix $C$ is $d = 0.0083$, which indicates that matrix $C$ can be regarded as fuzzy consensus judgment matrix. For the fuzzy consistent judgment matrix, its attribute weights are calculated according to equation (2). And a
judgment of $a$ has been given in literature [11]. The smaller $a$ is, the difference between the attributes needs to be taken seriously, while the larger $a$ is, the difference between attributes can be relatively ignored. In practical applications, it is generally accepted that $a=(n-1)/2$.

$$w_j = \frac{1}{n} - \frac{1}{2} + \frac{1}{n a} \sum_{j=1}^{n} c_j$$

(2)

Through calculation, for matrix $C$, $a=(n-1)/2=1.5$, so the weight value of the security attributes are $W_{\text{trans}}=0.233$, $W_{\text{recur}}=0.182$, $W_{\text{find}}=0.318$, $W_{\text{lost}}=0.267$. Then the security levels of the leaf nodes can be calculated by combining the weight values.

3.4. Security Situation Level Calculation

The security situation assessment method we adopt is to combine the security situation scores with the security attribute weight value of each leaf node. The calculation equation is as shown in equation (3).

$$R = W_{\text{trans}} \times S_{\text{trans}} + W_{\text{recur}} \times S_{\text{recur}} + W_{\text{find}} \times S_{\text{find}} + W_{\text{lost}} \times S_{\text{lost}}$$

(3)

In order to quantify the network security situation level of the internet of vehicles, we constructed the security situation level table of vehicle networks as shown in table 9.

| Security situation level | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| Safe                     | The network is normal, no serious security threats                          |
| Mildly dangerous         | The network is slightly affected and has a less destructive security threat |
| Generally dangerous      | The network is affected, and there are more destructive security threats,    |
|                          | causing moderate damage.                                                    |
| Moderately dangerous     | The network has been seriously damaged, jeopardizing the normal operation   |
|                          | of critical equipment and causing serious injury.                           |
| Highly dangerous         | The network was badly damaged, causing fatal damage to multiple cars        |

Then, by using equation (3), the security situation levels of each attack path in the three attack trees can be obtained. The results are respectively shown in table 10, table 11, and table 12. Based on the results obtained, the security situation level of the attack can be analyzed.

Table 9. Vehicle Network Security Situation Level

| Security situation level | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| Safe                     | The network is normal, no serious security threats                          |
| Mildly dangerous         | The network is slightly affected and has a less destructive security threat |
| Generally dangerous      | The network is affected, and there are more destructive security threats,    |
|                          | causing moderate damage.                                                    |
| Moderately dangerous     | The network has been seriously damaged, jeopardizing the normal operation   |
|                          | of critical equipment and causing serious injury.                           |
| Highly dangerous         | The network was badly damaged, causing fatal damage to multiple cars        |

Table 10. Security situation level of inner-vehicle network attack tree

| Node | Situation level | Node | Situation level | Node | Situation level |
|------|----------------|------|----------------|------|----------------|
| $E_{V1}$ | 3 | $E_{V5}$ | 4 | $E_{V9}$ | 4 |
| $E_{V2}$ | 3 | $E_{V6}$ | 4 | $E_{V10}$ | 4 |
| $E_{V3}$ | 4 | $E_{V7}$ | 3 | | |
| $E_{V4}$ | 3 | $E_{V8}$ | 4 | | |

Table 11. Security Situation Level of Vehicle Access Equipment Attack Tree

| Node | Situation level | Node | Situation level | Node | Situation level |
|------|----------------|------|----------------|------|----------------|
| $E_{D1}$ | 3 | $E_{D5}$ | 3 | $E_{D9}$ | 3 |
| $E_{D2}$ | 3 | $E_{D6}$ | 4 | $E_{D10}$ | 4 |
| $E_{D3}$ | 4 | $E_{D7}$ | 3 | $E_{D11}$ | 3 |
| $E_{D4}$ | 3 | $E_{D8}$ | 3 | | |

Table 12. Security Situation Level of Vehicle Network Communication Attack Tree

| Node | Situation level | Node | Situation level | Node | Situation level |
|------|----------------|------|----------------|------|----------------|
| $E_{T1}$ | 4 | $E_{T3}$ | 3 | $E_{T5}$ | 4 |
| $E_{T2}$ | 3 | $E_{T4}$ | 4 | $E_{T6}$ | 3 |
It can be concluded from the security situation level table that for the inner-vehicle network part, the security situation levels of the ECU and the gateway are higher. So these two parts need to be reinforced. For the vehicle access equipment part, the security level of the malicious command attack for the vehicle OBD diagnostic system is relatively high, and this system needs to be protected carefully. In the vehicle network communication part, the attack path with higher security situation level is spectrum interference attack and man-in-the-middle attack, indicating that the losses caused by these two types of attacks will be more serious, and early warning and security protection measures are supposed to be taken.

4. Comparison of Assessment Methods

We compare and analyze the results of the security situation levels using the AHP method and the FAHP method. Due to the large number of nodes in the attack tree, the attack path of the vehicle network communication attack tree is selected. To make the results clearer, the security attributes and security situation level used in the AHP method is consistent with the FAHP method. The comparative scales used are shown in table 13.

**Table 13. Comparison Scale**

| Scale       | Description                                                                 |
|-------------|-----------------------------------------------------------------------------|
| 1           | Attribute i and attribute j have the same effect on node score              |
| 3 (1/3)     | Attribute i has a slightly greater (smaller) impact on node scores than attribute j |
| 5 (1/5)     | Attribute i has a greater (smaller) impact on node score than attribute j   |
| 7 (1/7)     | Attribute i has a materially greater (smaller) impact on node scores than attribute j |
| 9 (1/9)     | The attribute i has extremely greater (smaller) impact on node score than attribute j |
| 2, 4, 6, 8  | Indicates the intermediate value of the above adjacent judgment             |

The four security attributes are compared according to table 13, and the judgment matrix is obtained as follows:

\[
C_{AHP} = \begin{pmatrix}
1 & 3 & 1/3 & 1/3 \\
1/3 & 1 & 1/3 & 1/7 \\
3 & 3 & 1 & 1/3 \\
1/3 & 1/2 & 1/3 & 1 \\
\end{pmatrix}
\]

Then the consistency ratio \( CR < 0.1 \) was used to test the consistency of the matrix. As in equation (4) \( CR \) is the ratio of the consistency index \( CI \) to the random consistency index \( RI \). The result of the judgment shows that \( C_{AHP} \) is a reasonable judgment matrix.

\[
CR = \frac{CI}{RI} < 0.1 \tag{4}
\]

In terms of calculating the security attribute weight, the matrix \( C_{AHP} \) is normalized according to the column using equation (5).

\[
\bar{a}_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} (i, j = 1, 2, ..., n) \tag{5}
\]

Then, the normalized judgment matrix is summed by rows, and normalized by equation (6) to calculate the weight of each security attributes.

\[
w_{ij} = \frac{\bar{w}_{ij}}{\sum_{j=1}^{n} \bar{w}_{ij}} \tag{6}
\]
Through calculation, the security attribute weights are: $W'_{\text{trans}} = 0.233$, $W'_{\text{recur}} = 0.182$, $W'_{\text{find}} = 0.31$, $W'_{\text{lost}} = 0.267$. By substituting these attribute weights into equation (3) for calculation and combining with table 9, the security situation level of each attack path calculated by AHP method can be obtained. The contradiction result of the two methods is shown in figure 4.

![Vehicle Network Communication Attack Tree](image)

**Figure 4. Vehicle Network Communication Attack Tree**

It can be concluded from the figure that the two methods have some differences in the judgment of the security situation level. However, experts generally believe that spectrum interference attack and DOS attack has a higher level of security situation, which can cause serious damages to the operation of the internet of vehicles and should be divides into moderately dangerous level. Therefore, the FAHP method adopted has higher accuracy than the AHP evaluation method. Besides, the FAHP method can more accurately reflect the security situation level in the internet of vehicles.

5. **Conclusion**

With the continuous development of the internet of vehicles, there will be various of cyber attacks. The research on the evaluation of the security threats of the internet of vehicles will become one of the research hotspots. We propose a vehicle network security situation assessment method based on attack tree and FAHP method. The attack trees of the inner-vehicle network, the vehicle access equipment, and the vehicle network communication are constructed respectively, and the security situation levels of the attack paths are evaluated. The use of FAHP method in the assessment reduces the impact of human subjective factors in this process, and improves the credibility of the vehicle network security situation assessment.

6. **Acknowledgments**

This work is supported in part by the Natural Science Foundation of Sichuan Province of China under Grant 2019YFG0201 and 2018GZDZX0011.

7. **References**

[1] Yegneswaran V, Barford P and Paxson V 2005 Using honeynets for Internet situational awareness. *Proc. of ACM Hotnets IV*

[2] Sabata B. and Ornes C 2006 Multi-source evidence fusion for cyber-situation assessment. Proceedings of Multisensor Multisource Information Fusion Conference pp 1-9

[3] Yin X, Yurcik W and Slagell A 2005 VisFlow connect-IP: An animated link analysis tool for visualizing netflows *Flocon*

[4] Chen X Z, Zhen Q H and Guan X H 2006 Quantitative hierarchical threat evaluation model for network security *Journal of Software* 17(4) pp 885-897

[5] Xu X H and Liu Z L 2005 A method for situation assessment based on D-S evidence theory *Electronics Optics & Control* 05 pp 36-37

[6] Hao S X, Xuan L and Zhang Z 2010 Algorithm of rule mining for network security situation prediction based on cloud *Computer and Digital Engineering* 38(8) pp 141-144
[7] Ren Q J, Pan G and Bai Y Q 2018 Security risk assessment of information system based on FAHP and attack tree Application of Electronic Technology 44(08) pp 113-117
[8] Li T, Li B, Chang C, et al 2018 Attack tree-based modeling of LoRaWAN security threat Communications Technology 51(11) pp 2695-2701
[9] Lv Z P, Qi W and Gu Z J 2018 Attack tree model based on fuzzy analytical hierarchy process Computer Engineering and Design 39(06) pp 1501-1505
[10] Song G X and Yang D L 2003 Consistency test and improvement method of fuzzy judgment matrix Systems Engineering 01 pp 110-116
[11] Yang Y H and Lv Y J 2018 Consistency Check of Fuzzy Judgment Matrix Statistics & Decision 34(04) pp 78-80
[12] Li F, Zhang H, Gao L, Wang J, Cesar Sanin & Edward Szczerbicki 2019 A Set of Experience-Based Smart Synergy Security Mechanism in Internet of Vehicles Cybernetics and Systems 50:2 pp 230-237
[13] Li F, Zhang H, Wang J, et al 2018 Toward Intelligent Vehicle Intrusion Detection Using the Neural Knowledge DNA Cybernetics & Systems pp 412-419